



Open Research Data

Rechtliche Grenzen und Gestaltungsmöglichkeiten

Prof. Dr. Florent Thouvenin

Dr. Stephanie Volz

unter Mitarbeit von:

MLaw Deborah De Col, RA und

MLaw Samuel Mätzler, RA

Zürich, 24. März 2025



Inhaltsverzeichnis

A.	Einleitung	5
1.	Auftrag	5
2.	Begriffe	5
B.	Grundlagen.....	6
1.	Rechte an Daten	6
1.1.	Kein Dateneigentum	6
1.2.	Urheberrecht	7
1.3.	Sui-Generis-Recht an Datenbanken in der EU	10
1.4.	Unmittelbare Übernahme von Arbeitsergebnissen (Art. 5 lit. c UWG)	12
1.5.	Schutz von Fabrikations- und Geschäftsgeheimnissen (Know-how).....	13
2.	Rechtsinhaberschaft	17
3.	Datenschutzrecht	19
C.	Schranken für ORD.....	21
1.	Fragestellung und Vorgehensweise	21
2.	Gesetzliche Schranken	22
2.1.	Exportkontrolle	22
2.2.	Informationssicherheitsrecht	24
2.3.	Gesundheitsrecht	25
2.3.1.	Allgemeines	25
2.3.2.	Humanforschungsbereich	26
2.3.3.	Nicht-Humanforschungsbereich	29
2.3.4.	Weitere Regelungen	29
2.4.	Gentechnik	30
2.5.	Umweltrecht	31
2.6.	Chemikalienrecht.....	33
2.7.	Lebensmittelrecht.....	33
2.8.	Energie- und Kernenergierecht.....	34
2.9.	Tierschutzrecht	35
2.10.	Finanzmarktrecht.....	36
3.	Rechte Dritter.....	37
3.1.	Urheberrechte	37
3.2.	Patente	38
3.3.	Ansprüche aus dem strafrechtlichen Geheimnisschutz	39
3.4.	Ansprüche aus UWG	39
3.5.	Datenschutzrechtliche Ansprüche	40
4.	Vertragliche Schranken	41
5.	Verantwortlichkeit	42



D.	Rechtliche Umsetzung von ORD	43
1.	Vorbemerkung	43
2.	Verfassungsrechtliche Rahmenbedingungen	44
2.1.	Für ORD relevante Grundrechte	44
2.2.	Einschränkung von Grundrechten	44
3.	Lizenzverträge	46
3.1.	Gegenstand	46
3.2.	Form	46
3.3.	Inhalt	47
4.	Kartellrechtliche Aspekte	48
5.	Lizenzen für ORD	49
5.1.	Abschluss	49
5.2.	Ausgestaltung	50
5.3.	Standardlizenzen	50
5.3.1.	Open Database License	51
5.3.2.	Creative Commons-Lizenzen	52
5.3.3.	Durchsetzung	53

EXECUTIVE SUMMARY

Die Rechte an Daten, die im Rahmen der dienstlichen Tätigkeit von Angestellten einer Institution des ETH-Bereichs geschaffen werden, stehen der jeweiligen Institution zu. Anderes gilt nur für Urheberrechte an in den Daten repräsentierten Werken der Literatur und Kunst. Damit können die Institutionen in der Regel bestimmen, wie und in welcher Form die Daten als ORD zugänglich zu machen sind. ORD unterliegt jedoch gewissen Schranken. Diese können sich aus gesetzlichen Vorgaben, Rechten Dritter oder vertraglichen Vereinbarungen ergeben.

Die Analyse möglicher gesetzlicher Schranken hat – ohne Anspruch auf Vollständigkeit – ergeben, dass namentlich im Exportkontrollrecht, Informationssicherheitsrecht, Gesundheitsrecht, Gentechnikrecht, Umweltrecht, Chemikalienrecht, Lebensmittelrecht, Energie- und Kernenergierecht sowie im Finanzmarktrecht Vorgaben zu finden sind, die dem Zugänglichmachen von Forschungsdaten als ORD entgegenstehen können. Neben gesetzlichen Schranken sind mögliche Rechte Dritter zu berücksichtigen. Besonders relevant sind dabei Urheberrechte, bspw. bei urheberrechtlich geschützten Bestandteilen eines Datensatzes oder bei gewissen Datenbanken, sowie Ansprüche aus dem Schutz von Fabrikations- und Geschäftsgeheimnissen (Art. 162 StGB und Art. 6 UWG), aus dem UWG (Art. 5 lit. c UWG) und Vorgaben des Datenschutzrechts.

Zudem können Verträge mit anderen Hochschulen oder Unternehmen Vorgaben zum Umgang mit Daten enthalten, insb. Geheimhaltungsverpflichtungen, die im Rahmen von ORD zu beachten sind.

Die Umsetzung einer ORD-Strategie muss sich am verfassungsrechtlichen Rahmen orientieren. Eine rechtliche Verpflichtung, Daten öffentlich zugänglich zu machen, kann die Wissenschaftsfreiheit, die Eigentumsfreiheit und die Wirtschaftsfreiheit tangieren und unter Umständen verletzen. Daneben können kartellrechtliche Vorgaben relevant sein, namentlich im Hinblick auf Zugangsverpflichtungen und eine mögliche Preisgestaltung.

Die Anbieter von ORD sind bei der Gestaltung der Lizenzverträge, die Dritten die Nutzung der Daten erlauben, rechtlich grundsätzlich frei. In individuellen Vereinbarungen können sie den Lizenznehmerinnen Verpflichtungen auferlegen, bspw. zur Zahlung einer Vergütung. Sinnvoll wird in der Regel aber die Nutzung von Standardlizenzen sein, insb. die «Creative Commons Zero License» (CC0) oder die «Creative Commons Attribution License» (CC-BY).

A. EINLEITUNG

1. Auftrag

Zum ETH-Bereich zählen sechs unabhängige Institutionen: die Eidgenössische Technische Hochschule Zürich (ETH Zürich), die Ecole polytechnique fédérale Lausanne (EPFL), das Paul Scherrer Institut (PSI), die Eidgenössische Materialprüfungs- und Forschungsanstalt (Empa), die Eidgenössische Forschungsanstalt für Wald, Schnee und Landschaft (WSL) und die Eidgenössische Anstalt für Wasserversorgung, Abwasserreinigung und Gewässerschutz (Eawag). Die zwei Schulen (ETH und EPFL) und die vier Forschungsanstalten (PSI, Empa, WSL und EAWAG) des ETH-Bereichs sind unabhängige Institutionen mit eigener Rechtspersönlichkeit. Ihre Tätigkeit wird durch das Bundesrecht geregelt.

Der ETH-Rat hat im Mai 2020 eine «*Open Research Data Position of the ETH Domain*» verabschiedet und ein «*Open Research Data Program*» begründet. Dieses Programm umfasst fünf Massnahmen. Massnahme vier betrifft die rechtlichen Grundlagen für Open Research Data (ORD). Im Rahmen dieser Massnahme werden drei Ziele verfolgt:

- Identifikation der (bundes-)rechtlichen Hindernisse beim Zugänglichmachen von Forschungsdaten als ORD durch die Forschenden bzw. die Institutionen des ETH-Bereichs;
- Klärung der Verantwortlichkeiten der Forschenden und der Institutionen des ETH-Bereichs;
- Entwicklung von ORD-Richtlinien, die im ETH-Bereich als gemeinsame Referenz verwendet werden können.

Das Center for Information Technology, Society, and Law (ITSL) der Universität Zürich wurde vom WSL Ende 2023 mit den Arbeiten zur Umsetzung von Massnahme vier beauftragt. Dieser Bericht untersucht die Fragestellungen, die sich aus den ersten beiden Zielen der Massnahme vier ergeben. Der Bericht beschränkt sich auf das Schweizer Bundesrecht; die einzige Ausnahme bildet das sog. sui-generis-Recht für Datenbanken der EU. Der Fokus der Analyse liegt auf Sachdaten. Da eine klare Trennung von Personen- und Sachdaten in vielen Fällen nicht möglich ist, werden Fragen des Datenschutzrechts aber mitberücksichtigt. Die Ausführungen zum Datenschutzrecht beschränken sich dabei auf das schweizerische Datenschutzgesetz (DSG), die Vorgaben der Datenschutzgrundverordnung (DSGVO) der EU werden nicht untersucht.

2. Begriffe

Dieser Bericht beruht auf den folgenden Begriffsdefinitionen:

- **Forschungsdaten** sind alle Daten, die von der relevanten wissenschaftlichen Gemeinschaft als notwendig erachtet werden, um Forschungsergebnisse zu validieren. Diese Daten können (und sollen) auch in anderen Forschungsprojekten verwendet werden. Der Begriff umfasst Rohdaten, bearbeitete Daten und Metadaten. Da die Rechtsordnung nicht allgemein, sondern nur in wenigen Erlassen nach diesen Datentypen unterscheidet, wird in diesem Bericht nur der umfassendere Begriff der Forschungsdaten verwendet.
- **FAIR-Prinzipien** sind international anerkannte Leitlinien zur Verbesserung der Auffindbarkeit, Zugänglichkeit, Interoperabilität und Wiederverwendbarkeit digitaler Inhalte.
- **Open Research Data (ORD)** sind Forschungsdaten, die den FAIR-Prinzipien entsprechen und öffentlich verfügbar, zugänglich und für mindestens 10 Jahre wiederverwendbar sind. Source Code wird von diesem Begriff grundsätzlich nicht erfasst. Anderes gilt nur, wenn Forschungsdaten ohne (spezifischen) Source Code nicht für die Validierung von Forschungsergebnissen oder für die Weiterverwendung in anderen Forschungsprojekten genutzt werden können. Zudem ist zu beachten, dass sich Forschungsdaten und Source Code nicht immer klar trennen lassen, so können bspw. die «weights» in trainierten Deep Neural Networks als Code oder als Daten angesehen werden.

B. GRUNDLAGEN

1. Rechte an Daten

1.1. Kein Dateneigentum

Die Frage, ob und unter welchen Voraussetzungen Forschungsdaten frei zugänglich gemacht werden können, hängt in grundlegender Weise von der Frage ab, ob die Daten «jemandem gehören», ob also Eigentumsrechte an Daten bestehen. Diese Frage kann, wenn sie so gestellt ist, klar beantwortet werden: Das Schweizer Recht kennt **kein Eigentum an Daten**, weder an Sachdaten noch an Personendaten.¹ Ein Eigentum im sachenrechtlichen Sinn besteht nur an Sachen. Eine Sache ist ein körperlicher, abgegrenzter, der menschlichen Herrschaft zugänglicher Gegenstand.² Daten fehlt es an der Körper-

¹ ROLF H. WEBER/FLORENT THOUVENIN, Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft?, ZSR 2018, 43 ff., 49; ALAIN SCHMID/KIRSTEN JOHANNA SCHMIDT/ZECH HERBERT, Rechte an Daten – zum Stand der Diskussion, sic! 2018, 627 ff., 629; STEPHAN WOLF/WOLFGANG WIEGAND, in: Geiser/Wolf (Hrsg.), Basler Kommentar Zivilgesetzbuch II, Art. 457-977 ZGB und Art. 1-61 SchIT ZGB, Basel 2023, Vor Art. 641 ff. N 19c.

² BSK ZGB II-WOLF/WIEGAND, Fn. 1, Vor Art. 641 ff. N 5 ff.; BARBARA GRAHAM-SIEGENTHALER, in: Aebi-Müller/Müller (Hrsg.), Berner Kommentar, Das Eigentum – Allgemeine Bestimmungen – Art. 641-654a ZGB, Bern 2022, Zweiter Abschnitt Sachen und andere Rechtsobjekte N 243.

lichkeit, weil sie nicht greifbar sind. Eine Sache ist bspw. ein Datenträger, nicht aber die auf diesem Träger gespeicherten Daten.

Dass es kein «Dateneigentum» gibt, bedeutet allerdings nicht, dass **an Daten** keine **anderen Rechte** bestehen können, die einer Nutzung oder dem freien Zugänglichmachen von Daten entgegenstehen würden. Solche Einschränkungen können sich insb. aus dem Urheberrecht, aus dem Schutz von Fabrikations- und Geschäftsgeheimnissen, aus dem Datenschutzrecht und in der EU auch aus dem sog. *sui generis* Schutz von Datenbanken ergeben.³

Möglich ist zudem eine **faktische Herrschaft über Daten**. Diese Herrschaft kann bspw. durch Speicherung in proprietären Systemen oder Verschlüsselung erfolgen. Möglich ist auch, dass die Herrschaft über Daten in einem Vertrag der einen oder anderen Partei zugewiesen wird. In diesen Fällen ist bisweilen von «*data ownership*» die Rede. Dieser Begriff kann hilfreich sein, um die faktische Herrschaft zum Ausdruck zu bringen. Er darf aber nicht darüber hinwegtäuschen, dass es sich bei dieser «ownership» nicht um Eigentum im Rechtssinn handelt. Immerhin wird die faktische Herrschaft bisweilen rechtlich abgesichert, namentlich durch den Schutz von Betriebs- und Geschäftsgeheimnissen (Art. 162 StGB und Art. 6 UWG).⁴

1.2. Urheberrecht

Das Urheberrecht schützt **Werke der Literatur und Kunst** (Art. 2 Abs. 1 URG). Dazu gehören unter anderem Texte, Musik, Filme, Bilder, Werke der Baukunst, Fotografien und Werke mit wissenschaftlichem Inhalt wie Zeichnungen, Pläne, Karten oder plastische Darstellungen (Art. 2 Abs. 2 URG). Als Werke gelten auch **Computerprogramme** (Art. 2 Abs. 3 URG). **Daten sind keine Werke der Literatur und Kunst** und damit nicht als solche urheberrechtlich geschützt. Wird ein **Werk der Literatur und Kunst** aber auf einem Datenträger gespeichert und damit **in Daten repräsentiert**, erfasst der urheberrechtliche Schutz des Werkes auch dessen Repräsentation in Form von Daten. Das Urheberrecht schützt Werke nur, wenn es sich um **geistige Schöpfungen** mit **individuellem Charakter** handelt (Art. 2 Abs. 1 URG). Eine Ausnahme besteht für Fotografien, die auch geschützt sind, wenn sie keinen individuellen Charakter haben (Art. 2 Abs. 3^{bis} URG). Zudem werden **bestimmte Leistungen** durch sog. Leistungsschutzrechte geschützt. Ein solcher Schutz besteht für Darbietungen von ausübenden Künstlern (Art. 33 ff. URG), bspw. Musiker, Schauspieler und Dirigenten, für die Hersteller von Ton- und Tonbildträgern (Art. 36 URG) und für Sendeunternehmen (Art. 37 URG). Diese Leistungsschutzrechte schützen die Darbietungen, Tonträger oder Sendung gegen die Nutzung durch Dritte.

³ Siehe dazu nachfolgend, B.1.3.

⁴ Siehe dazu nachfolgend, B.1.5.

Die **Schutzvoraussetzung** der **geistigen Schöpfung** bringt zum Ausdruck, dass nur von Menschen Geschaffenes ein Werk im Sinn des Urheberrechts sein kann.⁵ Nicht geschützt sind deshalb Werke, die von Computern selbstständig erzeugt werden, wohl aber Werke, die von Menschen mithilfe von Computern als Werkzeuge geschaffen wurden.⁶ Werke, die aufgrund einer menschlichen Eingabe (sog. prompt) selbstständig von Systemen der sog. generativen Künstlichen Intelligenz (KI) generiert werden, sind deshalb nicht urheberrechtlich geschützt.⁷ Anderes gilt, wenn KI als Werkzeug benutzt wird, um schöpferische Entscheidungen eines Menschen umzusetzen. Wo die Grenze zwischen einem weitgehend selbständigen Erstellen von Werken durch ein KI-System und der Nutzung eines solchen Systems als Werkzeug verläuft, lässt sich nur im Einzelfall bestimmen. Die Schutzvoraussetzung des **individuellen Charakters** ist eine qualitative Mindesthürde. Urheberrechtlich geschützt sind nur Werke, in denen ein gewisses Mass an Kreativität zum Ausdruck kommt. Damit unterscheiden sich geschützte Werke von banalen Schöpfungen und blossen Routinearbeiten. Der individuelle Charakter ergibt sich aus der Vielfalt der vom Urheber getroffenen Entscheidungen und aus überraschenden und ungewöhnlichen Kombinationen, die dazu führen, dass es ausgeschlossen erscheint, dass ein Dritter bei gleicher Aufgabenstellung das gleiche oder ein im Wesentlichen gleiches Werk geschaffen hätte.⁸

Als Werke gelten auch **Computerprogramme** (Art. 2 Abs. 3 URG). Urheberrechtlich geschützt ist dabei der Source Code, sofern er individuellen Charakter hat. Das ist nach der Lehre der Fall, wenn das Programm neu und nicht banal oder alltäglich ist.⁹ Wie bei den Werken der Literatur und Kunst sollte allerdings auch bei Computerprogrammen darauf abgestellt werden, ob es ausgeschlossen erscheint, dass ein Dritter bei gleicher Aufgabenstellung das gleiche oder ein im Wesentlichen gleiches Werk geschaffen hätte. Bei der Anwendung dürften sich allerdings keine Unterschiede gegenüber dem Text ergeben, ob das Programm banal oder alltäglich ist.

Urheberrechtlich geschützt sind auch **Sammelwerke**, wenn sie aufgrund der Auswahl oder Anordnung der Daten die Schutzvoraussetzungen des Urheberrechts erfüllen, also namentlich individuellen Charakter haben (Art. 4 Abs. 1 URG). Als Sammelwerke gelten auch **Datenbanken**. Datenbanken sind

⁵ BGE 130 III 168, E. 4.5 – «Bob Marley»; MANFRED REHBINDER/LORENZ HAAS/KAI-PETER UHLIG, in: Uhlig/Rehbinder/Haas (Hrsg.), Orell Füssli Kommentar, URG Urheberrechtsgesetz mit weiteren Erlassen und internationalen Abkommen, Zürich 2022 URG Art. 2 N 2; WILLI EGLOFF, in: Barrelet/Egloff (Hrsg.), Das neue Urheberrecht, Kommentar zum Bundesgesetz über das Urheberrecht (URG) und verwandte Schutzrechte, Kommentar, Bern 2020, Art. 2 N 8; RETO M. HILTY, Urheberrecht, Bern 2020, Rn. 151.

⁶ HILTY, Fn. 5, Rn. 152; ROLAND VON BÜREN, in: von Büren/David (Hrsg.), Schweizerisches Immaterialgüter- und Wettbewerbsrecht (SIWR), II/2, Urheberrecht im EDV-Bereich, Basel 1998, Rn. 403.

⁷ HILTY, Fn. 5, Rn. 152, 184; NATHALIE TISSOT/DANIEL KRAUS/VINCENT SALVADE, Propriété intellectuelle, Marques, brevets, droit d'auteur, Bern 2019, Rn. 16.

⁸ BGE 134 III 166, E. 2.3.2 – «Arzneimittel-Kompendium»; ebenso: BGE 142 III 387 E. 3.1 – «Fermeture d'une Terrasse»; BGE 136 III 225, E. 4.2 – «Guide orange».

⁹ URG Komm.-EGLOFF, Fn. 5, Art. 2 N 33, m.w.H.; OFK URG-REHBINDER/HAAS/UHLIG, Fn. 5, Art. 2 N 31; WILLI EGLOFF, FAIR Works – Eckpunkte eines Urheberrechts für digitale Welt, sic! 2022, 405 ff., 412.

damit geschützt, wenn sie aufgrund der Auswahl oder Anordnung der darin enthaltenen Daten individuellen Charakter haben.¹⁰ Diese Voraussetzung ist bei Datenbanken nicht leicht zu erfüllen. In der Regel sind jedenfalls nur strukturierte Datenbanken urheberrechtlich geschützt, weil es bei unstrukturierten Datenbanken an einer Anordnung der Daten fehlt, die den Schutz begründen können.¹¹ Die Auswahl der Daten dürfte für sich allein kaum je individuellen Charakter aufweisen und damit den urheberrechtlichen Schutz begründen können. Ein allfälliger urheberrechtlicher Schutz von Datenbanken bezieht sich immer nur auf die Auswahl und Anordnung der Daten, also sozusagen auf die **Struktur der Datenbank**, nicht auf die Daten als solche. Die einzelnen Daten – und auch die gesamte Menge der Daten – sind also urheberrechtlich nicht geschützt.

Zu beachten ist, dass das Urheberrecht nicht nur die ganzen Werke (also bspw. den ganzen Source Code), sondern **auch Teile** davon schützt (also bspw. Textteile, Sequenzen eines Source Code oder Teile einer Datenbank), wenn diese Teile für sich die Schutzvoraussetzungen erfüllen, also insb. individuellen Charakter haben (Art. 2 Abs. 4 URG).

Die Inhaber von Urheberrechten haben das ausschliessliche Recht zu bestimmen, ob, wann und wie das Werk verwendet wird (Art. 10 Abs. 1 URG). Teil dieses umfassenden Nutzungsrechts ist das sog. **Recht des Zugänglichmachens**, also das Recht, das Werk so zugänglich zu machen, dass Personen von Orten und zu Zeiten ihrer Wahl dazu Zugang haben (Art. 10 Abs. 2 lit. c URG). Dieses Recht erfasst das Zugänglichmachen von Werken über das Internet. Urheberrechtlich geschützte Werke dürfen damit grundsätzlich nur mit Zustimmung der Rechteinhaber als ORD zugänglich gemacht werden

Die Nutzung von urheberrechtlich geschützten Werken in der Forschung wird allerdings durch **Schranken** weitgehend freigestellt. Die Verwendung von Werken für die persönliche Forschung (bspw. das Verfassen einer Dissertation) wird durch die Schranke des Privatgebrauchs (Art. 19 Abs. 1 lit. a URG) freigestellt.¹² Die Vervielfältigung von Werken für die Forschung innerhalb einer Organisation kann als Betriebsgebrauch qualifiziert werden und ist damit ebenfalls freigestellt (Art. 19 Abs. 1 lit. c URG).¹³ Zudem enthält das URG eine explizite Schranke zugunsten der wissenschaftlichen Forschung, die es erlaubt, Werke zum Zweck der wissenschaftlichen Forschung zu vervielfältigen, wenn die Vervielfältigung durch die Anwendung eines technischen Verfahrens bedingt ist und zu den zu vervielfältigenden Werken ein rechtmässiger Zugang besteht (Art. 24d Abs. 1 URG). Das Zitieren von Werken wird zudem

¹⁰ EGLOFF, Fn. 5, URG 4 N 6; HILTY, Urheberrecht, Rn. 249; IVAN CHERPILLOD, in: Müller/Oertli (Hrsg.), Stämpfli Handkommentar, Urheberrechtsgesetz (URG), Bundesgesetz über das Urheberrecht und verwandte Schutzrechte. Mit Ausblick auf EU-Recht, deutsches Recht, Staatsverträge und die internationale Rechtsentwicklung, Bern 2012, Art. 4 N 4.

¹¹ EuGH GRUR 2009, 572; OGer ZH vom 1.9.1992, in: SMI 1993, 331 ff.; URG Komm.-EGLOFF, Fn. 5, Art. 4 N 6, m.w.H.

¹² BARRELET/EGLOFF, Fn. 5, Art. 19 N 11; SHK URG-Gasser, Fn. 10, Art. 19 N 21.

¹³ BARRELET/EGLOFF, Fn. 5, Art. 19 N 20; OFK URG-REHBINDER/HAAS/UHLIG, Fn. 5, Art. 19 N 31.

durch die Schranke der Zitatzfreiheit freigestellt (Art. 25 URG). Sind die Voraussetzungen einer dieser Schranken erfüllt, dürfen Werke und geschützte Leistungen auch ohne Zustimmung der Inhaber der Urheber- und Leistungsschutzrechte für die Forschung verwendet und insb. vervielfältigt, also bspw. auf einem Server gespeichert, werden. Diese Schranken erlauben es aber nicht, Werke als ORD auf einer Plattform zugänglich zu machen.

Der **Schutz** des Urheberrechts ist **befristet**. Er endet bei Werken der Literatur und Kunst 70 Jahre und bei Computerprogrammen 50 Jahre nach dem Tod des Urhebers. Bei Fotografien ohne individuellen Charakter endet der Schutz 50 Jahre nach der Herstellung (Art. 29 ff. URG). Der Schutz der Leistungen von ausübenden Künstlern endet 70 Jahre nach der Darbietung, der Schutz der Hersteller von Ton- und Tonbildträgern endet 70 Jahre nach Herstellung des Trägers. Der Schutz der Leistungen von Sendunternehmen endet 50 Jahre nach Ausstrahlung der Sendung (Art. 39 URG). Nach Ablauf des Schutzes fallen die Werke und Leistungen ins **Gemeingut (public domain)** und dürfen frei genutzt, also bspw. als ORD zugänglich gemacht, werden.

1.3. Sui-Generis-Recht an Datenbanken in der EU

Mit der **Richtlinie 96/9/EG über den rechtlichen Schutz von Datenbanken** (Datenbanken-RL) hat die damalige Europäische Gemeinschaft (EG) Mitte der 1990er Jahre einen Sonderschutz für Datenbanken geschaffen. Mit der Umsetzung der Datenbanken-RL haben alle Mitgliedstaaten der EG in ihrem nationalen Recht einen *urheberrechtlichen Schutz* von Datenbanken und ein sog. *sui-generis-Recht* für die Hersteller von Datenbanken geschaffen.¹⁴ Entstehung und Dauer des urheberrechtlichen Schutzes von Datenbanken bestimmt sich nach dem Urheberrecht. Das sui-generis-Recht entsteht mit dem Abschluss der Herstellung und endet nach 15 Jahren (Art. 10 Abs. 1 Datenbanken-RL).

Das **Schweizer Recht kennt kein sui-generis-Recht**, nur einen urheberrechtlichen Schutz von Datenbanken¹⁵. Datenbanken sind damit in der Schweiz nicht gegen die Entnahme und/oder Weiterverwendung der darin enthaltenen Daten geschützt. Das sui generis-Recht an Datenbanken ist beim Zugänglichmachen von Forschungsdaten als ORD dennoch zu beachten, weil die Daten weltweit (und damit auch in der EU) verfügbar gemacht werden und jede Form der öffentlichen Verfügbarmachung von Daten als Weiterverwendung gilt. Das Verfügbarmachen von Daten als ORD kann deshalb – unabhängig vom Standort des Servers – das sui generis-Recht an Datenbanken verletzen.

¹⁴ Art. 7 ff. Datenbanken-RL; zur Begründung insb. Erw. 38 Datenbanken-RL.

¹⁵ Siehe dazu vorne, B.1.2.

Zweck des sui-generis-Rechts an Datenbanken ist der Schutz der Investitionen der Hersteller von Datenbanken¹⁶. Als Datenbank gilt dabei eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen¹⁷, die **systematisch oder methodisch angeordnet** und einzeln mit elektronischen Mitteln oder auf andere Weise zugänglich sind (Art. 1 Abs. 2 Datenbanken-RL).¹⁸ Der Schutz erfasst damit nur strukturierte Datenbanken, keine unstrukturierten Datensammlungen.¹⁹ Voraussetzung für die Gewährung des Schutzes ist, dass der Hersteller in die Beschaffung, Überprüfung oder Darstellung des Inhalts einer Datenbank eine in qualitativer oder quantitativer Hinsicht erhebliche Investition getätigt hat. Als mit der Datenbank verbundene Investition gilt dabei allerdings nur derjenige Mitteleinsatz, welcher der Beschaffung oder der Zusammenstellung von Elementen dient, nicht die Investition in die Erzeugung dieser Elemente, also der Daten als solcher.²⁰

Das sui-generis-Recht vermittelt seinem Inhaber das Recht, Dritten die Entnahme und/oder Weiterverwendung der Gesamtheit oder eines in qualitativer und quantitativer Hinsicht wesentlichen Teils des Inhalts einer Datenbank zu untersagen.²¹ **Entnahme** bedeutet dabei die ständige oder vorübergehende Übertragung der Inhalte einer Datenbank auf einen anderen Datenträger, ungeachtet der dafür verwendeten Mittel und der Form der Entnahme (Art. 7 Abs. 2 Bst. a Datenbanken-RL). Als **Weiterverwendung** gilt jede Form der öffentlichen Verfügbarmachung (Art. 7 Abs. 2 Bst. b Datenbanken-RL).²² Von einem «wesentlichen Teil» kann ausgegangen werden, wenn im Verhältnis zum Gesamtvolumen der Datenbank ein quantitativ grosser Teil entnommen und/oder weiterverwendet wird. Ein qualitativ wesentlicher Teil liegt vor, wenn die Investition, die für das oder die entnommene(n) Element(e) getätigt worden ist, im Verhältnis zur Investition in die gesamte Datenbank erheblich ist.²³ Unzulässig ist auch die Entnahme und Weiterverwendung unwesentlicher Teile, sofern diese wiederholt und systematisch

¹⁶ EuGH vom 9. Oktober 2008, Rs. C-304/07 – Directmedia vs. Albert-Ludwigs-Universität, Rn. 33; EuGH vom 19. Dezember 2013, Rs. C-202/12, Innoweb vs. Wegener, Rn. 36 f.

¹⁷ EuGH vom 29. Oktober 2015, C-490/14 – Freistaat Bayern vs. Verlag Esterbauer GmbH, Rn. 17 und 22.

¹⁸ Nach dem EuGH muss es möglich sein, «jedes in der Sammlung enthaltene unabhängige Element zu lokalisieren», bspw. durch technische Mittel, einen Index, ein Inhaltsverzeichnis etc.; EuGH vom 9. November 2004, Rs. C-444/2 – Fixtures Marketing vs. OPAP, Rn. 30.

¹⁹ EuGH vom 1. März 2012, Rs. C-604/10, Rn. 30 und 32 – Football Dataco vs. Yahoo!.

²⁰ EuGH vom 09. November 2004, Rs. C-203/02 – British Horseracing vs. Hill Organization, Rn. 38; EuGH vom 9. November 2004, Rs. C-444/2 – Fixtures Marketing vs. OPAP, Rn. 39 ff., insb. 47; FLORENT THOUVENIN, Funktionale Systematisierung von Wettbewerbsrecht (UWG) und Immaterialgüterrecht, Diss. Zürich, Köln/Berlin/München 2007, 392.

²¹ THOUVENIN, Fn. 20, 393.

²² Nach dem EuGH umfassen «Entnahme» und «Weiterverwendung» jede unbefugte Nutzung einer Datenbank, die die Investition des Erstellers beeinträchtigt. EuGH vom 9. November 2004, Rs. C-203/02 – British Horseracing vs. Hill Organization, Rn. 51; HEIKO SENDROWSKI, Zum Schutzrecht «sui generis» an Datenbanken, GRUR 2005, 369 ff., 374.

²³ EuGH vom 5. März 2009, Rs. C-545/07 – Apis-Hristovich vs. Lakorda, Rn. 56 ff., insb. 59, 66 und 74; SENDROWSKI, Fn. 22, 375; ANDREAS WIEBE, Schutz von Maschinendaten durch das sui-generis-Schutzrecht für Datenbanken, GRUR 2017, 338 ff., 343 f.

erfolgt und einer normalen Nutzung der Datenbank durch den Hersteller entgegensteht oder dessen Interessen unzumutbar beeinträchtigt (Art. 7 Abs. 5 Datenbanken-RL).

Während das Urheberrecht die Auswahl und Anordnung der Daten in einer Datenbank, also deren Struktur, schützt²⁴, erfasst das sui-generis-Recht den **Inhalt von Datenbanken**, also eine Mehrheit von Daten, indem es die Entnahme einzelner oder mehrerer Elemente aus einer Datenbank erfasst, unabhängig davon, ob auch die Struktur der Datenbank übernommen wurde.²⁵ Der Hersteller einer Datenbank kann Dritten damit die Entnahme und Weiterverwendung der darin enthaltenen Daten in jeglicher Form verbieten, sofern es sich dabei um quantitativ oder qualitativ wesentliche Teile handelt. Das sui-generis-Recht vermittelt damit zwar Ausschliesslichkeitsrechte an Inhalten von Datenbanken und damit an gewissen Datenbeständen, nicht aber an einzelnen, in der Datenbank enthaltenen Daten.

1.4. Unmittelbare Übernahme von Arbeitsergebnissen (Art. 5 lit. c UWG)

Das UWG sieht nicht nur einen Schutz von Fabrikations- und Geschäftsgeheimnissen, sondern auch einen Tatbestand vor, der vor der unmittelbaren Übernahme von Arbeitsergebnissen schützt. Nach Art. 5 lit. c UWG handelt unlauter, wer das marktreife Arbeitsergebnis eines andern ohne angemessenen eigenen Aufwand durch technische Reproduktionsverfahren als solches übernimmt und verwertet. Dieser Tatbestand erfasst auch die unmittelbare Übernahme von Daten und vermag damit eine ähnliche Wirkung zu erzielen wie das sui-generis-Recht an Datenbanken.²⁶

Als **marktreifes Arbeitsergebnis** gilt nach Lehre und Rechtsprechung ein Produkt, das ohne weiteres Zutun gewerblich verwertet werden kann.²⁷ Dieses Arbeitsergebnis muss in irgendeiner Form materialisiert sein, weil es andernfalls gar nicht durch ein technisches Reproduktionsverfahren übernommen werden könnte.²⁸ Infrage kommen nicht nur körperliche, sondern auch unkörperliche Arbeitsergebnisse, bspw. Ton- und Bildaufnahmen, Computerprogramme oder Daten, die auf einem Datenträger gespeichert sind.²⁹ Das Tatbestandsmerkmal des **technischen Reproduktionsverfahrens** wurde weder vom Gesetzgeber noch von Lehre und Rechtsprechung näher definiert. Digitale

²⁴ Erw. 15 und 39 Datenbanken-RL.

²⁵ Siehe dazu auch Erw. 58 Datenbanken-RL, wonach das Urheberrecht die Struktur, das *Sui-generis*-Recht dagegen den Inhalt schützt; EuGH vom 5. März 2009, Rs. C-545/07 – Apis-Hristovich vs. Lakorda, Rn. 55.

²⁶ Siehe dazu vorne, B.1.3.

²⁷ FLORENT THOUVENIN, Art. 5 lit. c UWG – reloaded, sic! 2018, 595 ff., 598; BGE 131 III 384, 389 – «Suchspider».

²⁸ BGE 131 III 384, 389 – «Suchspider»; ähnlich auch ROLF H. WEBER/LENNART CHROBAK, in: Heizmann/Loacker (Hrsg.), Kommentar zum Bundesgesetz gegen den unlauteren Wettbewerb (UWG), Zürich/St. Gallen 2018, Art. 5 lit. c N 19.

²⁹ BGE 131 III 384, 389 f. – «Suchspider»; UWG-Komm.-WEBER/CHROBAK, Fn. 28, Art. 5 lit. c N 15, 18; SIMONE BRAUCHBAR BIRKHÄUSER, in: Jung (Hrsg.), Stämpfli Handkommentar, Bundesgesetz gegen den unlauteren Wettbewerb, Bern 2023, Art. 5 N 23; RETO ARPAGAU, in: Hilty/Arpagaus (Hrsg.), Basler Kommentar, Bundesgesetz gegen den unlauteren Wettbewerb (UWG), Basel 2013, Art. 5 N 31, 36.

Reproduktionsverfahren, bspw. das *web scraping* oder das Erstellen von digitalen Kopien von Daten,³⁰ sind aber zweifellos als technische Reproduktionsverfahren zu qualifizieren. Als **Übernahme** gilt eine Vervielfältigung, bei welcher das Arbeitsergebnis gegenständlich in den Vervielfältigungsvorgang einbezogen wird,³¹ als **Verwertung** jede gewerbliche Anwendung oder berufliche Nutzung im wirtschaftlichen Wettbewerb.³² Gemeint ist damit in erster Linie die Nutzung des übernommenen Arbeitsergebnisses zur Herstellung eines Konkurrenzproduktes. Nach einem Teil der Lehre und Rechtsprechung soll es aber bereits ausreichen, dass das Arbeitsergebnis als Grundlage einer eigenen Leistung verwendet wird.³³

Das Tatbestandsmerkmal des **angemessenen eigenen Aufwands** ist vom Gesetzgeber bewusst offen formuliert worden. Es soll erlauben, «den ungerechtfertigten Wettbewerbsvorteil des Zweitbewerbers abzuwägen» und die Amortisation «des Aufwandes des Erstkonkurrenten für die Schaffung des übernommenen Produkts» zu berücksichtigen.³⁴ Es ist allgemein anerkannt, dass der angemessene Aufwand im Rahmen eines sog. «doppelten Aufwandvergleichs» zu bestimmen ist.³⁵

Ob die Tatbestandsvoraussetzungen von Art. 5 lit. c UWG erfüllt sind, kann zwar nur im Einzelfall bestimmt werden. Die Bestimmung zeigt aber, dass die Übernahme von Daten Dritter auch dann einen Tatbestand des UWG verletzen kann, wenn diese Daten nicht geheim gehalten werden, sondern allgemein zugänglich sind.

1.5. Schutz von Fabrikations- und Geschäftsgeheimnissen (Know-how)

An Fabrikations- und Geschäftsgeheimnissen bestehen zwar keine Immaterialgüterrechte, Geheimnisse werden aber durch eine Reihe von Normen gegen Verrat und Nutzung durch Dritte geschützt. Diese Bestimmungen sanktionieren bei gegebenen Voraussetzungen **Eingriffe in die faktische Herrschaft über Daten** und dienen damit der rechtlichen Absicherung der tatsächlichen Kontrolle über Daten.³⁶ Im Vordergrund stehen die Bestimmungen von Art. 6 UWG und Art. 162 StGB.

³⁰ UWG Komm.-WEBER/CHROBAK, Fn. 28, 5 N 43; BSK UWG-ARPAGAU, Fn. 29, 5 N 84; so wohl auch SHK UWG-BRAUCHBAR BIRKHÄUSER, Fn. 29, Art. 5 N 33.

³¹ UWG Komm.-WEBER/CHROBAK, Fn. 28, Art. 5 lit. c N 23; ARNAUD NUSSBAUMER, in: Martenet/Pichonnaz (Hrsg.), *Commentaire Romand, Loi contre la concurrence déloyale (LCD)*, Basel 2017, Art. 5 N 68.

³² UWG Komm.-WEBER/CHROBAK, Fn. 28, Art. 5 lit. c N 25.

³³ BSK UWG-ARPAGAU, Fn. 29, Art. 5 N 74.

³⁴ Botschaft UWG, BBl 1983 1009, 1071.

³⁵ BGE 131 III 384, E. 4.3 – «Suchspider»; BGE 134 III 166, E. 4.3 – «Arzneimittelkompendium»; BGE 139 IV 17, E. 1.5 – «Cardsharing»; BSK UWG-ARPAGAU, Fn. 29, Art. 5 N 91; UWG Komm.-WEBER/CHROBAK, Fn. 28, Art. 5 lit. c N 47, 53.

³⁶ ALFRED FRÜH, *Datenzuordnung und Datennutzung*, digma 2019, 172 ff., 173.

Nach Art. 6 UWG handelt unlauter (und damit widerrechtlich), wer Fabrikations- oder Geschäftsgeheimnisse, die er ausgekundschaftet oder sonst wie unrechtmässig erfahren hat, verwertet oder anderen mitteilt. Als **Geheimnis** gilt die «besondere Kenntnis von Tatsachen, die nicht offenkundig oder allgemein zugänglich sind, an deren Geheimhaltung der Hersteller oder Geheimnisherr ein berechtigtes Interesse hat und die dieser tatsächlich geheim halten will».³⁷ Ein solches Geheimnis muss ausserdem einen potenziellen Einfluss auf das Geschäftsergebnis des Unternehmens haben, es muss mithin «fabrikations- oder geschäftsrelevant» sein, damit es vom Schutz von Art. 6 UWG erfasst ist.³⁸

Art. 6 UWG schützt allerdings nicht Unternehmensgeheimnisse an sich, sondern gewährt nur Ansprüche gegen die **Verwertung oder Mitteilung von Geheimnissen**, nachdem diese ausgekundschaftet oder auf eine andere Weise unrechtmässig in Erfahrung gebracht worden sind.³⁹ Nach einer solchen unzulässigen Kenntniserlangung ist gemäss Art. 6 UWG zusätzlich eine Handlung erforderlich, die objektiv geeignet ist, den Wettbewerb zu beeinflussen⁴⁰. Sind diese Voraussetzungen erfüllt, kann der Berechtigte den gesetzlich vorgesehenen Unterlassungs- und Beseitigungsanspruch (Art. 9 Abs. 1 lit. a und b UWG) geltend machen. Zudem bedroht Art. 23 Abs. 1 UWG die Verletzung von Art. 6 UWG auf Antrag mit Strafe.

Nach **Art. 162 StGB** wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft, wer ein Fabrikations- oder Geschäftsgeheimnis, das er infolge einer gesetzlichen oder vertraglichen Pflicht bewahren sollte, verrät, oder den Verrat für sich oder einen andern ausnützt. Der strafrechtliche Tatbestand ist mit Ausnahme der hier erforderlichen **vertraglichen oder gesetzlichen Geheimhaltungspflicht** weitgehend mit demjenigen von Art. 6 UWG identisch.⁴¹ Namentlich stimmt der Begriff des Fabrikations- und Geschäftsgeheimnisses in Art. 6 UWG mit demjenigen in Art. 162 StGB überein⁴².

Der Schutz von Fabrikations- und Geschäftsgeheimnissen durch Art. 6 UWG und Art. 162 StGB ist zeitlich nicht befristet, er kann also (theoretisch) ewig dauern. Der **Schutz endet** aber, sobald **die Information nicht mehr geheim** ist.⁴³

³⁷ BSK UWG-FRICK, Fn. 29, Art. 6 N 12; BGer 4A_78/2014 vom 23. September 2014, E. 11.1; OGer ZH UE140269 vom 19. März 2015, E. 2.c.

³⁸ SHK UWG-MABILLARD, Fn. 29, Art. 6 N 13; BSK UWG-FRICK, Fn. 29, Art. 6 N 15, je m.w.H.

³⁹ BSK UWG-FRICK, Fn. 29, Art. 6 N 5; SHK UWG-MABILLARD, Art. 6 N 21.

⁴⁰ SHK UWG-MABILLARD, Art. 6 N 21; BSK UWG-FRICK, Art. 6 N 53, je m.w.H.

⁴¹ MARCEL ALEXANDER NIGGLI/NADINE HAGENSTEIN, in: Niggli/Wiprächtiger (Hrsg.), Basler Kommentar, Strafgesetzbuch und Jugendstrafgesetzbuch (StGB/JStGB), Basel 2019, Art. 162 N 52; SHK UWG-MABILLARD, Fn. 38, Art. 6 N 5, m.w.H.

⁴² SHK UWG-MABILLARD, Fn. 38, Art. 6 N 8; BSK UWG-FRICK, Fn. 29, Art. 6 N 13; LORENZA FERRARI HOFER/DAVID VASELLA, in: Amstutz/Atamer (Hrsg.), Handkommentar zum Schweizer Privatrecht, Wirtschaftliche Nebenerlasse: FusG, UWG, KKG, PauRG und PrHG, Zürich 2023, Art. 6 N 3.

⁴³ SHK UWG-MABILLARD, Fn. 38, Art. 6 N 19; BSK UWG-FRICK, Fn. 29, Art. 6 N 51.

Ob **Forschungsdaten** nach Art. 6 UWG und Art. 162 StGB geschützt sind, wenn sie geheim gehalten werden, ist unklar. Wie ausgeführt, erfordert die Qualifikation als Fabrikations- oder Geschäftsgeheimnis, dass den geheimen Tatsachen ein gewisser **wirtschaftlicher Wert** zukommt bzw. dass die geheimen Tatsachen Auswirkungen auf das Unternehmensergebnis haben können.⁴⁴ Vor diesem Hintergrund wird in der Lehre vertreten, dass Informationen von wissenschaftlichem, universitärem Wert keine Geheimnisse i.S.v. Art. 6 UWG (und somit i.S.v. Art. 162 StGB) sind, solange sie nicht auf ein Unternehmen übertragen werden.⁴⁵ Andere Autoren erwähnen zwar (universitäre oder unternehmensinterne) Forschungs- und Entwicklungsarbeiten als Beispiele für Fabrikations- oder Geschäftsgeheimnisse, allerdings ebenfalls unter dem Vorbehalt, dass diese Arbeiten für die geschäftlichen Erfolge von Bedeutung und insofern von einer gewissen wirtschaftlichen Relevanz sind⁴⁶. Ein wirtschaftlicher Wert dürfte ohne Weiteres zu bejahen sein, wenn Hochschulen im Rahmen ihrer privatwirtschaftlichen Tätigkeit (Auftragsforschung für Unternehmen, Erstellen von Gutachten, etc.) Forschungsdaten generieren. Ob Forschungsdaten, die im Rahmen der «normalen» und damit grundsätzlich nicht-kommerziellen Forschung von Hochschulen geschaffen wurden, einen wirtschaftlichen Wert im Sinn von Art. 6 UWG und Art. 162 StGB haben – und damit dem Geheimnisschutz nach diesen Bestimmungen unterliegen – ist nach dem derzeitigen Stand von Literatur und Rechtsprechung unsicher.

Eine Auslegung nach Sinn und Zweck spricht allerdings dafür, **Forschungsdaten dem Schutz von Art. 6 UWG und Art. 162 StGB zu unterstellen**. Denn der Zweck dieser Bestimmungen ist darauf gerichtet, wirtschaftliche Einbussen aufgrund einer unbefugten Offenbarung und Verwertung von Geheimnissen zu verhindern. Auf diesen Aspekt ist die Geheimhaltung auch bei universitären Forschungsdaten ausgerichtet. Diese soll eine Kontrolle der Hochschule bzw. der Forschenden über ein zentrales Arbeitsergebnis ermöglichen und verhindern, dass Dritte (bspw. Unternehmen oder andere Forschende) durch die Nutzung der Forschungsdaten wirtschaftliche (oder anderweitige) Vorteile erzielen. Vor diesem Hintergrund drängt es sich auf, universitäre Forschungsdaten als Geschäftsgeheimnisse zu qualifizieren.

Forschungsdaten können damit zwar als **Geheimnisse im Sinn von Art. 6 UWG und Art. 162 StGB** qualifiziert werden. Das bedeutet aber nicht, dass das Zugänglichmachen von Forschungsdaten als ORD die Tatbestandsvoraussetzungen dieser Bestimmungen erfüllt. **Art. 6 UWG** erfasst nur das Verwerten oder Mitteilen von Geheimnissen, die der Betroffene ausgekundschaftet oder sonst wie unrechtmässig erfahren hat. Das ist beim Zugänglichmachen von Forschungsdaten als ORD in aller Regel

⁴⁴ Zum StGB: ANDREAS DONATSCH, in: Orell Füssli Kommentar StGB/JStGB, Mit weiteren Erlassen und Kommentar zu den Strafbestimmungen des SVG, BetmG, AIG und OBG, Zürich 2022, Art. 162 N 3; BSK StGB-NIGGLI/HAGENSTEIN, Fn. 41, Art. 162 N 9; STEPHAN SCHLEGEL, in: Wohlers/Godenzi/Schlegel (Hrsg.), Handkommentar, Schweizerisches Strafgesetzbuch, Bern 2020, Art. 162 N 3.

⁴⁵ BSK UWG-FRICK, Fn. 29, Art. 6 N 15.

⁴⁶ OFK StGB-DONATSCH, Fn. 44, Art. 162 N 3.

nicht der Fall, weil die Forschenden im Rahmen ihrer Forschungsarbeiten Zugang zu den Daten erhalten oder diese selbst generiert haben. Anderes gilt nur, wenn sich Forschende unrechtmässig Zugang zu den Daten verschafft haben. Möglich ist aber ein Verstoss gegen **Art. 162 StGB**. Dies setzt voraus, dass eine **gesetzliche oder vertragliche Pflicht** besteht, ein Geheimnis zu bewahren. Dem Zugänglichmachen von Forschungsdaten als ORD können namentlich Geheimhaltungspflichten entgegenstehen, die sich insb. aus Verträgen ergeben, die im Rahmen von Forschungsk Kooperationen mit Unternehmen (oder anderen Forschungsinstitutionen) abgeschlossen werden.⁴⁷ Solche Verträge werden oft schon im Vorfeld der eigentlichen Kooperation geschlossen, bspw. in Form von Geheimhaltungsvereinbarungen (NDA) oder Materialtransfervereinbarungen (MTA). Diese Verträge haben in der Praxis eine grosse Bedeutung. Für Forschungsk Kooperationen mit Unternehmen (oder anderen Forschungsinstitutionen) ist zentral, dass die vertraglichen Vorgaben eingehalten werden, nicht nur, aber insb. die Vorgaben zur Geheimhaltung. Werden die Daten entgegen einer vertraglichen Pflicht zur Geheimhaltung als ORD zugänglich gemacht, liegt nicht nur eine Vertragsverletzung, sondern auch ein Verstoss gegen Art. 162 StGB und damit eine strafbare Handlung vor. Dieses Vergehen wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. Zur Antragstellung berechtigt ist dabei der Geheimnisherr.⁴⁸

Weitere Straftatbestände zum Schutz von Geheimnissen finden sich im Schweizer Recht unter den strafbaren Handlungen gegen die Amts- und Berufspflicht, namentlich die Verletzung des **Amtsgeheimnisses** (Art. 320 StGB). Der Geheimnisbegriff ist ähnlich wie derjenige bei Art. 6 UWG und Art. 162 StGB zu verstehen. Als Geheimnisse gelten auch nach Art. 320 StGB alle nicht allgemein bekannten oder zugänglichen Informationen, deren Schutz vor Preisgabe der Berechtigte will und an deren Geheimhaltung ein objektives Interesse besteht.⁴⁹ Ein Geheimnis wird zum Amtsgeheimnis, wenn die geheim zu haltende Tatsache dem Amtsträger in seiner Eigenschaft als Beamter anvertraut worden ist oder er diese aufgrund seiner amtlichen Stellung wahrgenommen hat.⁵⁰ Es braucht mit anderen Worten einen Kausalzusammenhang zwischen der Kenntnisnahme des Geheimnisses und der amtlichen Funktion. Ob **universitäre Forschungsdaten** dieses Kriterium erfüllen, wurde – soweit ersichtlich – in der Lehre und/oder Rechtsprechung noch nicht diskutiert. Entsprechend bedarf die Norm der Auslegung. Der Wortlaut von Art. 320 StGB («anvertraut worden ist» und «wahrgenommen hat») deutet darauf hin, dass nur geheime Tatsachen erfasst werden, die bereits existieren, und von denen der oder die Beamte im Rahmen seiner oder ihrer behördlichen Tätigkeit Kenntnis erhält. Nicht erfasst

⁴⁷ Siehe dazu unten, C.4.

⁴⁸ BSK StGB-NIGGLI/HAGENSTEIN, Fn. 41, Art. 162 N 56 f.; OFK StGB-DONATSCH, Fn. 44, Art. 162 N 8.

⁴⁹ BSK StGB-OBERHOLZER, Fn. 41, Art. 320 N 8; OFK StGB-ISENRING, Fn. 44, Art. 320 N 3, je m.w.H.

⁵⁰ Kasuistik: Patientendossier der SUVA (BGE 142 IV 65, E. 5.2); sämtliche Informationen im Zusammenhang mit einem Strafverfahren (BGer 6B_439/2016 vom 21. April 2017, E. 2.2.2); Einträge im Strafregister (BGE 127 IV 122, E. 1).

sind dagegen Erkenntnisse bzw. Tatsachen, die im Rahmen der behördlichen Tätigkeit hervorgebracht bzw. generiert werden. Forschungsdaten, die im Rahmen von universitären Forschungsarbeiten entstehen, sind damit nicht vom Begriff des Amtsgeheimnisses erfasst. Für dieses Ergebnis spricht auch eine Auslegung nach Sinn und Zweck der Bestimmung. Diese dient in erster Linie der Wahrung von Geheimnissen, an denen ein öffentliches Interesse (bspw. Geheimhaltung der aussenpolitischen Strategie der Schweiz) oder ein Individualinteresse besteht (bspw. Strafregistereinträge), und die in amtlicher Eigenschaft wahrgenommen worden sind. Auch wenn es Konstellationen gibt, in denen öffentliche oder private Interessen an der Geheimhaltung von Forschungsdaten bestehen, dient die Geheimhaltung von Forschungsdaten nicht (primär) dem Schutz der Interessen Dritter, sondern dem Schutz der Interessen der Forschenden und Forschungsinstitutionen an der Kontrolle der im Rahmen der Forschung generierten Daten und an deren wissenschaftlichen oder wirtschaftlichen Verwertung. Bei den Forschungsdaten, die von öffentlichen Forschungseinrichtungen – bspw. den Institutionen des ETH-Bereichs – im Rahmen ihrer Forschung generiert wurden, handelt es sich damit um Geschäftsgeheimnisse (in einem weiteren Sinn) und nicht um Amtsgeheimnisse.

2. Rechtsinhaberschaft

Soweit Rechte an Daten bestehen, stellt sich die Frage, wem diese Rechte zustehen. Die Immaterialgüterrechtsgesetze regeln nur die Frage des originären Erwerbs und stellen klar, dass Immaterialgüterrechte übertragen, also auch derivativ erworben werden können. Diese Gesetze regeln aber (mit Ausnahme von Art. 17 URG) nicht, wem die Rechte an Immaterialgütern im Verhältnis zwischen Arbeitgeber und Arbeitnehmendem zustehen. Im privatrechtlichen Arbeitsverhältnis wird diese Frage für das Patent- und Designrecht in Art. 332 OR geregelt; für das Urheberrecht hat der Gesetzgeber die Frage (ausser für Computerprogramme in Art. 17 URG) bewusst nicht geregelt. Im Verhältnis zwischen den Forschenden und den Institutionen des ETH-Bereichs wird die Frage in Art. 36 ETH-Gesetz geregelt.

Art. 36 Abs. 1 ETH-Gesetz lautet: «Mit Ausnahme der Urheberrechte gehören den ETH und den Forschungsanstalten alle Rechte an Immaterialgütern, die von Personen in einem Arbeitsverhältnis nach Artikel 17 in Ausübung ihrer dienstlichen Tätigkeit geschaffen worden sind.»

Der Gesetzeswortlaut und die Ausführungen in der Botschaft stellen klar, dass die Bestimmung alle spezialgesetzlich normierten Immaterialgüter erfasst, also namentlich Erfindungen, Werke der Literatur und Kunst, Designs, Marken, Topographien von Halbleitererzeugnissen und Pflanzensorten.⁵¹ Weder das Gesetz noch die Botschaft äussern sich zu Rechten an Daten, die nicht immaterialgüterrechtlich

⁵¹ Botschaft ETH-Gesetz, BBl 2002 3465 ff., 3495.

geschützt sind. Auch die bei Daten im Vordergrund stehende Berechtigung an Geschäftsgeheimnissen wird nicht direkt angesprochen. Die Botschaft stellt allerdings klar, dass an den Institutionen des ETH-Bereichs «im grossem Umfang wirtschaftlich verwertbares Know-how geschaffen» werde und das Ziel der Revision von Art. 36 ETH-Gesetz «eine klare Zuweisung der Rechte an sämtlichen Immaterialgütern im ETH-Bereich» sei.

Daten sind, wie ausgeführt, keine Sachen,⁵² sondern **immaterielle Güter**.⁵³ Art. 36 ETH-Gesetz sieht vor, dass den Institutionen des ETH-Bereichs mit Ausnahme der Urheberrechte **«alle Rechte an Immaterialgütern»** gehören, die von Arbeitnehmenden dieser Institutionen bei Ausübung ihrer dienstlichen Tätigkeit geschaffen worden sind. Auch in der Marginalie von Art. 36 ETH-Gesetz wird nicht der Begriff «Immaterialgüterrechte», sondern «Immaterialgüter» verwendet. Der Wortlaut der Bestimmung spricht damit für einen umfassenden Anwendungsbereich, der alle Immaterialgüter und nicht nur die spezialgesetzlich geregelten Immaterialgüterrechte erfasst – und damit auch allfällige Rechte an Daten.

Zum gleichen Ergebnis führt eine Auslegung nach Sinn und Zweck der Regelung, zumal der Bundesrat gemäss Botschaft **«eine klare Zuweisung der Rechte an sämtlichen Immaterialgütern im ETH-Bereich»** schaffen wollte. Dass der Arbeitgeber an den Gütern berechtigt ist, die seine Arbeitnehmenden bei Ausübung ihrer dienstlichen Tätigkeit schaffen, ist bei Sachen derart selbstverständlich, dass die Frage im Arbeitsrecht gar nicht geregelt wird. Eine gesetzliche Regelung besteht nur für Immaterialgüterrechte – und dort wird die Frage, ausser für das vom sog. Schöpferprinzip dominierte Urheberrecht, durchwegs durch eine Zuweisung an den Arbeitgeber gelöst. Und selbst im Urheberrecht sieht die einzige gesetzliche Regelung, die allerdings nur für Computerprogramme gilt, eine Zuweisung der Rechte an den Arbeitgeber vor (Art. 17 URG). Dasselbe gilt nach Art. 36 Abs. 2 Satz 1 ETH-Gesetz für die Institutionen des ETH-Bereichs.

Daten werden, wie ausgeführt, nur teilweise und nur indirekt durch spezialgesetzlich geregelte Immaterialgüterrechte geschützt.⁵⁴ Sie werden aber vom **Schutz von Fabrikations- und Geschäftsgeheimnissen** in Art. 6 UWG und Art. 162 StGB erfasst, wenn sie die Voraussetzungen der Qualifikation als Geheimnis erfüllen.⁵⁵ Auch der Schutz von Fabrikations- und Geschäftsgeheimnissen vermittelt **Rechte an den geheimen Informationen**. Diese sind, wie die Immaterialgüterrechte, als subjektive Rechte zu qualifizieren.⁵⁶ Im *common law* wird der Schutz von *«trade secrets»* denn auch als

⁵² Siehe dazu vorne, B.1.1.

⁵³ FLORENT THOUVENIN, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, SJZ 113/2017, 21 ff., 25.

⁵⁴ Siehe dazu vorne, B.1.2.

⁵⁵ Siehe dazu vorne, B.1.5.

⁵⁶ THOUVENIN, Fn. 20, 560 f.; SHK UWG-MABILLARD, Fn. 29, Art. 6 N 1, m.w.H.

Immaterialgüterrecht (*intellectual property right*) verstanden.⁵⁷ Dieses Verständnis liegt auch dem TRIPS-Agreement zugrunde, das auch die Schweiz unterzeichnet und ratifiziert hat.⁵⁸ Damit bestehen durchaus valable Gründe, die Rechte an geheimen Informationen, welche der Schutz von Fabrikations- und Geschäftsgeheimnissen den Geheimnisherrn vermittelt, als Immaterialgüterrechte zu qualifizieren, zumal es sich um subjektive Rechte an immateriellen Gütern handelt. Ob diese Gründe für das Schweizer Recht zu überzeugen vermögen, kann hier offen bleiben. Denn Daten sind unzweifelhaft Immaterialgüter im Sinn von Art. 36 ETH-Gesetz. Die Rechte an Daten werden damit von dieser Bestimmung erfasst und die Rechtsinhaberschaft an den Daten den Institutionen des ETH-Bereichs zugewiesen.

Die Auslegung von Art. 36 ETH-Gesetz führt damit zum Ergebnis, dass die **Rechte an Daten**, welche die Arbeitnehmenden der Institutionen des ETH-Bereichs in Ausübung ihrer dienstlichen Tätigkeit schaffen, diesen Institutionen gehören.

3. Datenschutzrecht

Das Datenschutzgesetz (DSG) regelt die Bearbeitung von **Personendaten natürlicher Personen** (Art. 2 Abs. 1 DSG). Als Personendaten gelten alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (Art. 5 lit. a DSG). Der Begriff der Personendaten ist damit äusserst weit gefasst. Auch der Begriff der **Bearbeitung** ist äusserst weit. Er erfasst jeden Umgang mit Personendaten, wozu insb. das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Offenlegen, Archivieren, Löschen und Vernichten der Daten gehören (Art. 5 lit. d DSG). Das DSG hat damit einen äusserst weiten Anwendungsbereich und erfasst auch viele Forschungsdaten, die als ORD auf über das Internet zugänglich gemacht werden.

Nicht erfasst wird die Bearbeitung von **anonymisierten Daten und Sachdaten** (bspw. Daten über den Verschleiss einer Flugzeugturbine), die von Anfang an keinen Personenbezug aufweisen. Bei der Anonymisierung werden Personendaten so weit verändert, dass der Bezug zu einer bestimmten Person

⁵⁷ ONLY ANSGAR, Harmonising the Protection of Trade Secrets: Challenges and Perspectives, in: Werra (Hrsg.), La protection des secrets d'affaires / The Protection of Trade Secrets, Zürich 2013, 32; MARCO BRONCKERS/NATHALIE M. McNELIS, Is the EU obliged to improve the protection of trade secrets? An inquiry into TRIPS, the European Convention on Human Rights and the EU Charter of Fundamental Rights, EIPR 2012, 673 ff., 677.

⁵⁸ ONLY ANSGAR, Harmonising the Protection of Trade Secrets: Challenges and Perspectives, in: Werra (Hrsg.), La protection des secrets d'affaires / The Protection of Trade Secrets, Zürich 2013, 33; INGO MEITINGER, Die globale Rahmenordnung für den Schutz von Geschäftsgeheimnissen im TRIPS-Abkommen der WTO und ihre Auswirkungen auf die Rechtslage in der Schweiz, sic! 2002, 145 ff., 147.

nicht mehr oder nur noch mit einem unverhältnismässig grossen Aufwand hergestellt werden kann.⁵⁹ Wann Personendaten als anonymisiert gelten, ist allerdings bis heute nicht genügend geklärt. Unklar ist namentlich, ab welchem Abstrahierungsgrad eine Re-Identifizierung als unverhältnismässig aufwändig erscheint. Zudem ist aus technischer Sicht umstritten, inwiefern eine Anonymisierung überhaupt möglich ist. Gerade die Entwicklungen im Bereich von KI und Big Data erlauben immer einfachere Rückschlüsse von vermeintlich anonymisierten Datensätzen auf bestimmte oder bestimmbar Personen.

Als Bundesorgane dürfen die Institutionen des ETH-Bereichs Personendaten nur bearbeiten, wenn dafür eine **gesetzliche Grundlage** besteht. Das ist der Fall. Nach Art. 36c Abs. 1 ETH-Gesetz können die ETH und die Forschungsanstalten im Rahmen von Forschungsprojekten Personendaten, einschliesslich besonders schützenswerter Personendaten, bearbeiten, soweit dies für das entsprechende Projekt erforderlich ist. Bei der Bearbeitung von Personendaten müssen die Institutionen des ETH-Bereichs die Vorgaben des DSG einhalten. Das wird in Art. 36c Abs. 2 ETH-Gesetz ausdrücklich erwähnt, ergibt sich aber bereits aus dem DSG, weil die Institutionen des ETH-Bereichs datenschutzrechtlich als Bundesorgane zu qualifizieren sind (Art. 2 Abs. 1 lit. b i.V.m. Art. 5 lit. i DSG).

Nach Art. 39 DSG dürfen Bundesorgane Personendaten für **nicht personenbezogene Zwecke**, insb. für Forschung, Planung oder Statistik, bearbeiten, wenn vier Voraussetzungen erfüllt sind: (i) die Daten werden anonymisiert werden, sobald der Bearbeitungszweck dies erlaubt; (ii) das Bundesorgan gibt privaten Personen besonders schützenswerte Personendaten nur so bekannt, dass die betroffenen Personen nicht bestimmbar sind; (iii) die Empfängerin oder der Empfänger gibt Dritten die Daten nur mit der Zustimmung des Bundesorgans weiter, das die Daten bekanntgegeben hat; und (iv) die Ergebnisse werden nur so veröffentlicht, dass die betroffenen Personen nicht bestimmbar sind. Diese Vorgaben gelten auch für die Forschung an den Institutionen des ETH-Bereichs. Art. 36c Abs. 1 ETH-Gesetz bildet lediglich die gesetzliche Grundlage, die erforderlich ist, *damit* diese Institutionen im Rahmen der Forschung Personendaten bearbeiten dürfen; Art. 39 DSG enthält spezifische Vorgaben, *wie* die Bearbeitung zu erfolgen hat.

Die Voraussetzungen von Art. 39 DSG zielen zwar auf die Veröffentlichung von Forschungsergebnissen in wissenschaftlichen Publikationen, sie gelten aber auch für die **Veröffentlichung von Forschungsdaten**. Das Erfordernis der Anonymisierung wird in Art. 39 DSG gleich zweimal erwähnt: bei der Bearbeitung der Daten in (i) und bei der Publikation der Ergebnisse in (iv). Damit ist klar, dass (i) Personendaten bei der Bearbeitung für die Forschung sobald als möglich anonymisiert werden müssen

⁵⁹ BEAT RUDIN, in: Baeriswyl/Pärli/Blonski (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz (DSG), Bern 2021, Art. 5 N 13; GABOR P. BLECHTA/LUCA DAL MOLIN/KIRSTEN WESIACK-SCHMIDT, in: Blechta/Vasella (Hrsg.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz (DSG/BGÖ), Basel 2024, Art. 5 N 35.

und (ii) nur in anonymisierter Form veröffentlicht werden dürfen. **Personendaten dürfen damit nur in anonymisierter Form als ORD zugänglich gemacht werden.**

C. SCHRANKEN FÜR ORD

1. Fragestellung und Vorgehensweise

Beim Zugänglichmachen von Forschungsdaten als ORD sind die Vorgaben des geltenden (objektiven) Rechts einzuhalten und es ist zu prüfen, ob Dritte (subjektive) Rechte (bspw. Urheberrechte oder vertragliche Ansprüche) geltend machen können, die dem Zugänglichmachen von Forschungsdaten als ORD entgegenstehen.

Unter dem Titel «**Gesetzliche Schranken**» wird untersucht, ob das Bundesrecht gesetzliche Vorgaben enthält, die dem Zugänglichmachen von Forschungsdaten als ORD entgegenstehen. Um diese sehr weit gefasste Frage zu beantworten, wurde in einem ersten Schritt ermittelt, welche Bundesgesetze Normen enthalten könnten, die dem Zugänglichmachen von Forschungsdaten durch die Institutionen des ETH-Bereichs entgegenstehen. Die Auswahl der potenziell relevanten Erlasse wurde durch den Regelungsbereich der jeweiligen Bundesgesetze und die Tätigkeitsbereiche der Institutionen des ETH-Bereichs definiert. Die Liste der potenziell relevanten Erlasse wurde an mehreren Sitzungen mit Vertretern aller Institutionen des ETH-Bereichs auf Relevanz und Lücken überprüft. Dabei sind keine zusätzlichen Regelungsbereiche ersichtlich geworden, die ebenfalls zu untersuchen wären.

Angesichts der **umfassenden Fragestellung** ist aber davon auszugehen, dass das Bundesrecht weitere Bestimmungen enthält, die dem Zugänglichmachen von Forschungsdaten als ORD entgegenstehen, die durch unser Vorgehen nicht identifiziert werden konnten und deshalb in diesem Bericht nicht berücksichtigt wurden. Die Forschenden und/oder die Rechtsabteilungen der Institutionen des ETH-Bereichs werden deshalb jeweils **für einen konkreten Datensatz prüfen müssen, ob es Bestimmungen gibt, die dem Zugänglichmachen der Daten entgegenstehen**. Die Beurteilung dieser konkreten Frage dürfte in der Regel durchaus möglich sein, weil die Forschenden und/oder die Rechtsabteilungen der jeweiligen Institutionen mit den Normen vertraut sein werden, die für den jeweiligen Forschungsbereich relevant sind.

Aufgrund des skizzierten Vorgehens wurden die folgenden Regelungsbereiche identifiziert und untersucht: Exportkontrollrecht, Informationssicherheitsrecht, Gesundheitsrecht, Gentechnikrecht, Umweltrecht, Chemikalienrecht, Lebensmittelrecht, Energie- und Kernenergierecht, Tierschutzrecht sowie Finanzmarktrecht. Wie erwähnt, ist davon auszugehen, dass es weitere Regelungsbereiche gibt, die Bestimmungen enthalten, die dem Zugänglichmachen von Forschungsdaten als ORD entgegenstehen.

Die nachfolgenden Ausführungen dürfen deshalb **nicht als abschliessende Darstellung aller gesetzlichen Schranken von ORD** verstanden werden.

Unter dem Titel **«Rechte Dritter»** wird geprüft, welche (subjektiven) Rechte Dritter und welche vertraglichen Verpflichtungen einer Veröffentlichung und Wiederverwendung von Forschungsdaten als ORD entgegenstehen können.

2. Gesetzliche Schranken

2.1. Exportkontrolle

Für Forschungsdaten können Ausfuhrbeschränkungen gelten. Güter sind gemäss Güterkontrollgesetz (GKG)⁶⁰ neben physischen Waren auch Software und Technologien, d.h. Informationen, die der Entwicklung, Herstellung oder Verwendung eines Gutes dienen, jedoch weder allgemein zugänglich sind noch aus der wissenschaftlichen Grundlagenforschung stammen (Art. 3 lit. d GKG).

Forschungsinstitutionen müssen die Vorgaben⁶¹ der Exportkontrolle einhalten. Der Export von Forschungsdaten kann im Einzelfall eine Genehmigung erfordern oder ganz verboten sein. Ob derartige Beschränkungen gelten, bestimmt sich nach dem Inhalt der Forschungsdaten und dem Empfängerland. Werden Forschungsdaten als ORD zur Verfügung gestellt, ist die Exportkontrolle besonders schwierig, weil der Transfer an den Grenzen nicht physisch kontrolliert werden kann und die Daten grundsätzlich weltweit zugänglich gemacht werden.

Enthalten die Forschungsdaten Informationen zur Herstellung von sensiblen Gütern, ist ihr Export immer genehmigungspflichtig. Sensible Daten sind nach Art. 3 lit. b GKG nicht nur Daten aus der Rüstungstechnologie, sondern zahlreiche auf den ersten Blick harmlose Daten, sofern diese auch zu militärischen Zwecken genutzt werden können (Dual-Use-Güter). Dual-Use-Güter bzw. die Parameter für deren Qualifikation werden in der Liste der Güter mit doppeltem Verwendungszweck aufgeführt, die in den Anhängen 1 und 2 der Güterkontrollverordnung (GKV)⁶² enthalten ist. Grundsätzlich handelt es sich dabei um Güter mit doppeltem Verwendungszweck, die ursprünglich für einen zivilen Einsatz-

⁶⁰ Bundesgesetz über die Kontrolle zivil und militärisch verwendbarer Güter, besonderer militärischer Güter sowie strategischer Güter, SR 946.202.

⁶¹ In der Schweiz kommen im Zusammenhang mit der Exportkontrolle eine Reihe von Erlassen zur Anwendung, namentlich das Güterkontrollgesetz (GKG), die Güterkontrollverordnung (GKV), die Verordnung über die Ausfuhr und Vermittlung von Gütern zur Internet- und Mobilfunküberwachung (VIM), das Embargogesetz (EmbG), das Kriegsmaterialgesetz (KMG) und die einschlägigen Güterlisten. Darüber hinaus gibt es internationale Vereinbarungen: Vertrag über den Waffenhandel (Arms Trade Treaty [ATT]); Vereinbarung von Wassenaar (Wassenaar Arrangement [EWA]); Chemiewaffenübereinkommen (CWÜ).

⁶² Verordnung über die Kontrolle zivil und militärisch verwendbarer Güter, besonderer militärischer Güter sowie strategischer Güter, SR 946.202.1.



bereich erstellt wurden, aber aufgrund ihrer Eigenschaften auch für militärische Zwecke verwendet werden können. Beispiele sind Informationen aus dem Bereich der Telekommunikation, Elektronik, Chemie, Schiffstechnik oder Verschlüsselungstechnik. Ein zentrales Merkmal von Dual-Use-Gütern – im Gegensatz zu den besonderen militärischen Gütern oder dem Kriegsmaterial – ist, dass ihr Einsatzbereich bzw. ihre Endverwendung oft nicht klar ist. Im Anhang 3 GKV ist aufgelistet, was für einen Kriegseinsatz notwendig ist, bspw. Informationen zur Herstellung chemischer oder biologischer Agenzien, zugehörige Ausrüstung oder die Verwendung radioaktiver Stoffe.

Das GKG findet Anwendung auf den Export von Forschungsdaten, die noch nicht öffentlich zugänglich sind. Nicht anwendbar ist es beim Export von Forschungsdaten, die bereits allgemein bekannt und zugänglich sind. Allgemein zugänglich sind Informationsquellen, wenn sie technisch geeignet und bestimmt sind, der Allgemeinheit Informationen zu verschaffen. Für Forschungsdaten bedeutet dies insb., dass bereits publizierte oder allgemein bekannte Daten (bspw. in einer wissenschaftlichen Publikation) keinen exportkontrollrechtlichen Schranken unterstehen und deshalb als ORD veröffentlicht werden können.

Die Schranken der Exportkontrolle gelten nicht für Informationen aus der wissenschaftlichen Grundlagenforschung. Gemäss Anhang 1 GKV handelt es sich bei der Grundlagenforschung um «[...] experimentelle oder theoretische Arbeiten hauptsächlich zur Erlangung von neuen Erkenntnissen über grundlegende Prinzipien von Phänomenen oder Tatsachen, die nicht in erster Linie auf ein spezifisches praktisches Ziel oder einen spezifischen praktischen Zweck gerichtet sind».

Die Art und Weise des Exports von Technologie und Software ist aus Sicht des GKG unerheblich. Um die Rechtsfolgen des GKG auszulösen, genügt es, dass die Güter an den Kunden im Ausland gelangen. Die Begriffe Ausfuhr und Durchfuhr erfassen damit auch die nicht-gegenständliche Übermittlung, bspw. über Datenleitungen. Ungeklärt ist die Frage, wie es sich verhält, wenn die Daten nicht exportiert, sondern auf einem sich in der Schweiz befindlichen Server zum Herunterladen bereitgestellt werden. Zumindest wenn der Zugang zu den Forschungsdaten über Repositorien erfolgt und sich die Empfänger vor dem Herunterladen der Daten registrieren müssen, lässt sich nachvollziehen, in welches Zielland die Forschungsdaten gelangen und ein Export in bestimmte Länder kann verhindert werden. Ein Missbrauch durch Umgehung der Registrierung kann allerdings nicht ausgeschlossen werden. Welche Sicherheits- und Kontrollmechanismen beim Zugänglichmachen von Forschungsdaten als ORD über Repositorien erforderlich sind, wurde bisher aus rechtlicher Sicht nicht näher untersucht und ist unklar.

Damit kann festgehalten werden, dass bei Forschungsdaten, die als ORD veröffentlicht werden sollen, nach Massgabe der exportkontrollrechtlichen Vorgaben geprüft werden muss, ob sie genehmigungspflichtige oder verbotene Informationen oder Software enthalten.

Die Prüfung muss im Einzelfall für die konkreten Daten vorgenommen werden. Forschungsdaten, die nach dem GKG verbotene Informationen enthalten, dürfen nicht als ORD zugänglich gemacht werden. Damit genehmigungspflichtige Forschungsdaten als ORD veröffentlicht werden können, muss für alle Länder eine Ausfuhrbewilligung eingeholt werden, wenn der Zugang zu ORD uneingeschränkt von allen Ländern aus möglich sein soll.

Ausgeschlossen ist folglich die Veröffentlichung von Forschungsdaten als ORD, wenn diese Daten als Dual-Use-Güter zu qualifizieren sind. Die Qualifikation der Forschungsdaten als Dual-Use-Güter erfolgt anhand der Liste der Güter mit doppeltem Verwendungszweck in den Anhängen 1 und 2 der GKV.

2.2. Informationssicherheitsrecht

Forschungsdaten können Informationen enthalten, die aus Sicht des Staates als sensibel einzuschätzen sind. Solche Informationen können unter das Informationssicherheitsgesetz (ISG) fallen, was deren Nutzung als ORD beschränkt.

Das ISG soll die sichere Bearbeitung von Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz von Informatikmitteln des Bundes gewährleisten (Art. 1 Abs. 1 ISG). Es dient dem Schutz unterschiedlicher öffentlicher Interessen, etwa der Entscheidungs- und Handlungsfähigkeit der Behörden und der inneren und äusseren Sicherheit der Schweiz (Art. 1 Abs. 2 ISG). Verpflichtet wird durch das ISG u.a. die Bundesverwaltung, was auch die dezentralen Verwaltungseinheiten nach Massgabe ihrer Organisationserlasse umfasst.⁶³ Die Institutionen des ETH-Bereichs sind dezentrale Verwaltungseinheiten und damit vom ISG erfasst (siehe Anhang 1: Liste der Verwaltungseinheiten der Bundesverwaltung, B., VI., Ziff. 2.2.5-2.2.10 Regierungs- und Verwaltungsorganisationsverordnung).

Das ISG sieht vor, dass der Bundesrat die Geltung des Gesetzes auf diejenigen Organisationen der dezentralen Bundesverwaltung einschränken kann, die sicherheitsempfindliche Tätigkeiten ausüben oder zur Ausübung ihrer Aufgaben Informatikmittel des Bundes einsetzen oder darauf zugreifen (Art. 2 Abs. 3 ISG). Von dieser Möglichkeit hat der Bundesrat in der Informationssicherheitsverordnung (ISV) Gebrauch gemacht und in Art. 2 Abs. 2 ISV zugleich klargestellt, welche Bestimmungen des ISG für diese dezentralen Einheiten der Bundesverwaltung gelten. Das Eidgenössische Departement für Wirtschaft, Bildung und Forschung (WBF) hat mit Schreiben vom 17. Dezember 2024 bestätigt, dass keine der dezentralen Einheiten des WBF – und damit keine Institutionen des ETH-Bereichs – ständig sicherheitsempfindliche Tätigkeiten ausüben. Die Institutionen des ETH-Bereichs sind damit nicht vollumfänglich dem ISG unterstellt. Das ISG ist aber anwendbar, wenn Institutionen des ETH-Bereichs

⁶³ So die Botschaft zum Bundesgesetz über die Informationssicherheit vom 22. Februar 2017, BBl 2017 2953 ff., 3012. Siehe auch Art. 2 Abs. 3 Regierungs- und Verwaltungsorganisationsgesetz (RVOG), welcher dies ausdrücklich festhält.

klassifizierte Informationen des Bundes bearbeiten oder Informatikmittel des Bundes einsetzen oder darauf zugreifen (Art. 2 Abs. 3 ISG i.V.m. Art. 2 Abs. 2 ISV).

Gemäss ISG werden Informationen als «intern» klassifiziert, wenn deren Kenntnisnahme durch Unberechtigte die öffentlichen Interessen «beeinträchtigen» kann (siehe Art. 13 Abs. 1 ISG). Als «vertraulich» werden Informationen klassifiziert, wenn deren Kenntnisnahme durch Unberechtigte die öffentlichen Interessen «erheblich beeinträchtigen» kann (siehe Art. 13 Abs. 2 ISG). Als «geheim» zu klassifizieren sind Informationen, wenn deren Kenntnisnahme durch Unberechtigte die öffentlichen Interessen «schwerwiegend beeinträchtigen» kann (siehe Art. 13 Abs. 3 ISG). Erfüllen Informationen die Kriterien nach Art. 13 ISG nicht, so sind sie nicht klassifiziert und unterstehen in der Schweiz keinen besonderen rechtlichen Vorgaben, sofern es sich nicht um Personendaten handelt oder spezifische Bestimmungen greifen (wie etwa für Amtsgeheimnisse). Sind sie jedoch klassifiziert, so sind die entsprechenden Informationen nicht frei zugänglich. Zugang erhalten nur Personen, die Gewähr bieten, dass sie mit den Informationen sachgerecht umgehen und sie zur Erfüllung einer gesetzlichen Aufgabe benötigen und ggf. über eine vertraglich vereinbarte Zugangsberechtigung verfügen (Art. 14 Abs. 1 lit. a ISG). Dies kann eine Verwendung als ORD verunmöglichen.

Die Vorgaben sind für den ETH-Bereich und andere dezentrale Verwaltungseinheiten in den Ausführungsbestimmungen der Informationssicherheitsverordnung (ISV) konkretisiert. Als Grundsatz gilt, dass die Bekanntgabe und das Zugänglichmachen klassifizierter Informationen auf das Minimum zu beschränken ist (Art. 16 Abs. 1 ISV). Die einzelnen Verwaltungseinheiten erlassen zudem regelmässig Weisungen (bspw. die Research Data Management Guidelines der ETH) in denen sie eigene, auf ihren Bereich zugeschnittene Anforderungen und Konkretisierungen an die Informationssicherheit festlegen.⁶⁴

Da klassifizierte Informationen definitionsgemäss nur einem eingeschränkten Personenkreis zur Verfügung stehen dürfen, ist ein Zugänglichmachen solcher Informationen als ORD ausgeschlossen.

2.3. Gesundheitsrecht

2.3.1. Allgemeines

Die Daten des Gesundheitsbereichs sind in der Schweiz stark reguliert. Heikle Daten – oft solche mit Personenbezug – sind in diesem Sektor eher die Regel als die Ausnahme. Die betroffenen Personen sind besonders vulnerabel, namentlich wenn zur Datenerhebung auf ihren Körper eingewirkt wird, etwa

⁶⁴ Die ETH Zürich hat dies bspw. in ihrer Weisung «Informationssicherheit an der ETH Zürich» vom 9. April 2018 gemacht.

anlässlich von Blutabnahmen. Ausserdem besteht eine kaum auflösbare Informationsasymmetrie zwischen Ärzt:innen oder Forschenden und Patient:innen.

Medizinische Fachleute und ihre Hilfspersonen unterstehen deshalb dem strafrechtlich geschützten Berufsgeheimnis (Art. 321 Strafgesetzbuch; StGB), das ihnen die Offenbarung von Berufsgeheimnissen ohne Einwilligung der Patient:in untersagt. Die Verletzung von Berufsgeheimnissen in der Forschung am Menschen ist ebenfalls strafbewehrt (Art. 321^{bis} StGB). Als vorherrschendes Prinzip kommt dem sog. *informed consent* (informierte Einwilligung) im Gesundheitsrecht grosse Bedeutung zu. Da das Gesundheitswesen in der Schweiz primär Sache der Kantone ist, untersteht die klassische medizinische Versorgung in erster Linie dem kantonalen Recht (bspw. kantonale Gesundheitsgesetze). Auf weitere Ausführungen zu Rechtsfragen der medizinischen Versorgung wird hier deshalb verzichtet.

2.3.2. *Humanforschungsbereich*

Die Forschung ist in vielen Bereichen massgeblich auf die Nutzung von Daten aus dem Gesundheitsbereich angewiesen. Dem Bund wurde deshalb mit Art. 118b BV die Kompetenz übertragen, Vorschriften über die Forschung am Menschen zu erlassen, «soweit der Schutz seiner Würde und seiner Persönlichkeit es erfordert» (Abs. 1 Satz 1). Der Bund hat dabei die Forschungsfreiheit zu wahren und der Bedeutung der Forschung für Gesundheit und Gesellschaft Rechnung zu tragen (Abs. 1 Satz 2).

Auf dieser Grundlage hat der Bund das **Humanforschungsgesetz (HFG)** erlassen. Dieses findet auf sämtliche «Forschung zu Krankheiten des Menschen sowie zu Aufbau und Funktion des menschlichen Körpers» Anwendung, u.a. wenn biologisches Material oder gesundheitsbezogene Personendaten verwendet werden (Art. 2 Abs. 1 lit. d und e HFG). Unter diesen Begriff der Forschung kann neben jeglicher medizinischer Forschung⁶⁵ auch Forschung zur Prävention von Unfällen oder Sportverletzungen oder Forschung der Gesundheitspsychologie fallen, sowie sozial- und geisteswissenschaftliche Forschung, die sich mit dem Zusammenhang zwischen sozialen Bedingungen und spezifischen Krankheiten oder gesellschaftlichen Auswirkungen von Krankheiten befasst.⁶⁶ Auch für klinische Versuche mit Heilmitteln ist das HFG anwendbar (Art. 53 Heilmittelgesetz). Ob das HFG Anwendung findet, ist im Einzelfall zu prüfen.

⁶⁵ Diese befasst sich gemäss BENEDIKT VAN SPYK, in: Rütsche (Hrsg.), Stämpfli's Handkommentar, Humanforschungsgesetz (HFG), Bundesgesetz vom 30. September 2011 über die Forschung am Menschen, Bern 2015, Art. 3 N 16 etwa mit den physischen und psychischen Ursachen von Krankheiten (Grundlagenforschung); der Übertragung von Grundlagenerkenntnissen auf den klinischen Bereich (translationale Forschung); der Entstehung, dem Verlauf, der Diagnose, Prophylaxe sowie Behandlung von Krankheiten (klinische Forschung); der Häufigkeit und Verteilung von Krankheiten in der Gesellschaft (epidemiologische Forschung).

⁶⁶ SHK HFG-VAN SPYK, Fn 65, Art. 3 N 19.

Im Kontext von ORD sind die besonderen Vorschriften für gesundheitsbezogene Personendaten relevant. Das HFG regelt nicht nur die Erhebung der Daten, etwa anlässlich von Forschungsprojekten mit Personen (in Form von Befragungen oder Beobachtungen), sondern auch die sekundäre Nutzung, d.h. die **Weiterverwendung** solcher Daten. Der Begriff der Weiterverwendung wird dabei sehr weit verstanden. Erfasst wird jeder Umgang zu Forschungszwecken mit bereits entnommenem biologischem Material und mit bereits erhobenen Daten (Art. 24 Humanforschungsverordnung [HFV]).⁶⁷

Das HFG unterscheidet zwischen der Weiterverwendung von biologischem Material und genetischen Daten einerseits (Art. 32 HFG) und nichtgenetischen gesundheitsbezogenen Personendaten andererseits (Art. 33 HFG). Für deren Weiterverwendung gelten je nach Kategorie unterschiedliche Vorgaben, die nachfolgend kurz skizziert werden:

Biologisches Material und genetische Daten dürfen gemäss Art. 32 Abs. 1 HFG in *unverschlüsselter* Form für *ein* Forschungsprojekt weiterverwendet werden, wenn die betroffene Person nach hinreichender Aufklärung eingewilligt hat. Sind das Material und die Daten dagegen *verschlüsselt* (pseudonymisiert), d.h. mit einer bestimmten Person über einen Schlüssel verknüpft (siehe Art. 3 lit. h HFG), und somit nur für diejenigen Personen bestimmbar, welche die verschlüsselten Informationen entschlüsseln können, so darf eine Weiterverwendung *zu Forschungszwecken generell* erfolgen, wenn die betroffene Person nach hinreichender Aufklärung eingewilligt hat (Art. 32 Abs. 2 HFG; sog. Generalkonsent). Sollen biologisches Material und genetische Daten *anonymisiert* und anschliessend *zu Forschungszwecken generell* weiterverwendet werden, muss die betroffene Person vorgängig informiert werden und sie darf der Anonymisierung nicht widersprochen haben (Art. 32 Abs. 3 HFG).⁶⁸

Bei nichtgenetischen gesundheitsbezogenen Daten sind die Möglichkeiten der Weiterverwendung weitergehend. Sie dürfen in *unverschlüsselter* Form *zu Forschungszwecken generell* weiterverwendet werden, wenn die betroffene Person nach hinreichender Aufklärung eingewilligt hat (Art. 33 Abs. 1 HFG; Generalkonsent). Sind die Daten *verschlüsselt*, so ist die Weiterverwendung *zu Forschungszwecken generell* zulässig, sofern die betroffene Person vorgängig informiert wurde und sie nicht widersprochen hat (Art. 33 Abs. 2 HFG).⁶⁹

⁶⁷ Die Verordnung nennt ausdrücklich das Beschaffen, Zusammenführen oder Sammeln, das Registrieren oder Katalogisieren, das Aufbewahren oder Erfassen in Bio- oder Datenbanken sowie das Zugänglichmachen, Bereitstellen oder Übermitteln biologischen Materials oder gesundheitsbezogener Personendaten.

⁶⁸ Siehe zum Ganzen: SAMUEL MÄTZLER, Datenschutz in der (Human-)Forschung: Grundlagen und Probleme bei der Sekundärnutzung von Personendaten, in: Jusletter vom 30. Januar 2023, Rn. 44.

⁶⁹ Siehe zum Ganzen: MÄTZLER, Fn. 68, Rn. 45.

Die Weiterverwendung von anonym erhobenen und anonymisierten gesundheitsbezogenen Daten fällt nicht in den Anwendungsbereich des HFG und ist deshalb voraussetzungslos zulässig.⁷⁰ Dies bezieht sich indes nur auf die Weiterverwendung von bereits erhobenen Daten.

Nach Art. 34 HFG dürfen biologisches Material oder gesundheitsbezogene Personendaten ausnahmsweise zu Forschungszwecken weiterverwendet werden, wenn es (1) unmöglich oder unverhältnismässig schwierig ist, die Einwilligung einzuholen bzw. über das Widerspruchsrecht zu informieren, oder dies unzumutbar ist; (2) keine dokumentierte Ablehnung vorliegt; und (3) das Interesse der Forschung gegenüber dem Interesse der betroffenen Person, über die Weiterverwendung ihres biologischen Materials und ihrer Daten zu bestimmen, überwiegt (Art. 34 lit. a-c HFG).

Wird mit dem Material bzw. den Daten ein Forschungsprojekt durchgeführt, das unter das HFG fällt, so ist dieses stets bewilligungspflichtig (Art. 45 Abs. 1 lit. a HFG). Findet eine Weiterverwendung gestützt auf Art. 34 HFG statt, ist ebenfalls stets eine Bewilligung notwendig (Art. 45 Abs. 1 lit. b HFG).

Die Bewilligung wird dabei von der zuständigen Kantonalen Ethikkommission erteilt, welche die ethischen, rechtlichen und wissenschaftlichen Anforderungen des HFG kontrolliert und insb. überprüfen muss, ob der Schutz der betroffenen Personen gewährleistet ist (Art. 51 Abs. 1 HFG). Zuständig ist dabei die Ethikkommission des Kantons, in dessen Gebiet die Forschung durchgeführt wird (Art. 47 Abs. 1 HFG). Eine eidgenössische Ethikkommission existiert für den Humanforschungsbereich nicht; auch Bundesbehörden sind gegenüber einer Kantonalen Ethikkommission rechenschaftspflichtig.

Daten, die unter das HFG fallen und somit einen Personenbezug aufweisen, dürfen bereits gestützt auf das DSG nicht als ORD zugänglich gemacht werden. Für das HFG sind zusätzlich einschränkend die besonderen Vorschriften für die Weiterverwendung einzuhalten. Der Begriff der Weiterverwendung umfasst auch das Aufbewahren oder Erfassen in Bio- oder Datenbanken (Art. 24 lit. c HFV) und das Zugänglichmachen, Bereitstellen oder Übermitteln von biologischem Material oder gesundheitsbezogenen Personendaten (Art. 24 lit. d HFV). Entsprechend sind auch für solche Handlungen die Art. 32-34 HFG einzuhalten, wobei keine Bewilligung durch die Ethikkommission notwendig ist, solange die Weiterverwendung nicht im Rahmen eines konkreten Forschungsprojekts erfolgt (so etwa bei einer blossen Aufbewahrung in einer Datenbank).

Daten ohne Personenbezug sind nicht vom HFG erfasst und können damit grundsätzlich als ORD zugänglich gemacht werden. Dabei ist zu beachten, dass bei genetischen Daten (und biologischem Material) selbst für den **Vorgang der Anonymisierung** eine vorgängige **Informationspflicht** besteht und die Anonymisierung nur zulässig ist, wenn die betroffene Person nicht von ihrem Widerspruchsrecht Gebrauch gemacht hat.

⁷⁰ SHK HFG-RUDIN, Fn. 65, Art. 33 N 18.

2.3.3. Nicht-Humanforschungsbereich

Auf Forschung mit anonymisiertem biologischem Material (Art. 2 Abs. 2 lit. b HFG) und mit anonym erhobenen oder anonymisierten gesundheitsbezogenen Daten (Art. 2 Abs. 2 lit. c HFG) ist das HFG nicht anwendbar. Die entsprechenden Daten sind im Schweizer Recht grundsätzlich unreguliert. Werden allerdings Personendaten bearbeitet, ohne dass der Anwendungsbereich des HFG eröffnet ist, so gelten die allgemeinen datenschutzrechtlichen Vorgaben für die Bearbeitung von Personendaten.⁷¹ Diese lassen die Bearbeitung zu nicht personenbezogenen Zwecken, insb. für die Forschung unter gewissen Voraussetzungen zu (Art. 31 Abs. 2 lit. e DSG für Private; Art. 39 DSG für Bundesbehörden), nicht aber das Zugänglichmachen nicht anonymisierter Daten als ORD.⁷²

Sowohl bei Personendaten als auch bei anonymisierten Daten spielen *soft law* und wissenschaftliche Standards eine zentrale Rolle. Viele Fachzeitschriften und Forschungsförderungsinstitutionen verlangen auch für Forschungsprojekte, die nicht unter das HFG fallen, den Nachweis der ethischen Vertretbarkeit. Damit müssen faktisch auch bei solchen Daten gewisse Vorgaben befolgt werden. Diese Vorgaben können sich auch auf die Verwendung von ORD erstrecken. Eine Prüfung erfolgt i.d.R. durch Ethikkommissionen von Forschungsinstitutionen, etwa durch die Ethikkommission der ETH Zürich.⁷³ Diese Prüfung findet aber nur statt, wenn keine (rechtlich verbindliche) Prüfung durch die Kantonale Ethikkommission erfolgen muss.

Aus rechtlicher Sicht gelten somit einzig die Vorgaben des DSG: Die Daten dürfen damit nur in anonymisierter Form als ORD zugänglich gemacht werden. Es ist allerdings denkbar, dass Fachzeitschriften und Forschungsförderungsinstitutionen weitergehende Anforderungen stellen.

2.3.4. Weitere Regelungen

In Spezialgesetzen bestehen weitere Vorgaben, die auf ORD einen Einfluss haben können. Besondere Regelungen existieren bspw. für genetische Untersuchungen beim Menschen. Art. 10 des Bundesgesetzes über genetische Untersuchungen beim Menschen (GUMG)⁷⁴ sieht bspw. vor, dass Proben und genetischen Daten durch angemessene technische und organisatorische Massnahmen vor unbefugtem Umgang und unbefugter Bearbeitung zu schützen sind. Das Transplantationsgesetz (TxG) erlaubt hingegen die Veröffentlichung von Daten von allgemeinem Interesse, die sich auf die Anwendung des Gesetzes beziehen (Art. 59 Abs. 3 TxG). Einschränkend wird allerdings festgehalten, dass die

⁷¹ Siehe dazu vorne, 0.

⁷² Siehe dazu vorne, 0.

⁷³ Siehe dazu <<https://ethz.ch/de/die-eth-zuerich/organisation/gremien-gruppen-kommissionen/ethikkommission-on.html>> (zuletzt besucht am 27. Mai 2024).

⁷⁴ SR 810.12.

betroffenen Personen nicht bestimmbar sein dürfen. In den Verordnungen wird sodann festgelegt, dass bestimmte Personendaten zu Forschungszwecken Dritten in anonymisierter Form bekanntgegeben werden können, es sei denn die betroffene Person habe in die Bekanntgabe eingewilligt oder es liege eine Bewilligung der zuständigen Ethikkommission nach Art. 45 HFG vor (siehe Art. 34^m Organzuteilungsverordnung und Art. 49^h Abs. 2 Transplantationsverordnung; ebenso Art. 76 Strahlenschutzverordnung). Im Bereich der Arzneimittel sind dagegen auch Berichte über die Ergebnisse klinischer Versuche zwingend zu anonymisieren (Art. 73 Abs. 1 Arzneimittelverordnung). Insgesamt ist die Verwendung solcher Daten als ORD angesichts dieser strengen Vorgaben kaum denkbar, zumal regelmässig auf die (ebenfalls strengen) Vorgaben des HFG verwiesen wird.

Neben Einschränkungen können spezialgesetzliche Regelungen auch die Nutzung bestimmter Daten ermöglichen, etwa indem sie einen Datenzugang vorsehen. Gestützt auf das Krebsregistrierungsgesetz (KRG) können bspw. Daten zu Forschungszwecken zur Verfügung gestellt werden (Art. 23 Abs. 2 KRG). Das KRG verweist dabei für die Erhebung oder Weiterverwendung ebenfalls auf das HFG (Art. 23 Abs. 4 KRG). Dies ermöglicht zwar die Nutzung der Daten zu Forschungszwecken, aber kein Zugänglichmachen als ORD.

Einige Erlasse sehen indes auch das Zugänglichmachen als ORD explizit vor, etwa in Form von *Open Government Data* (OGD). Art. 21 Abs. 4 des Bundesgesetzes über die Krankenversicherung (KVG) legt fest, dass das zuständige Bundesamt die für die Erfüllung der Aufgaben nach dem KVG erforderlichen Daten den Datenlieferanten, der Forschung und Wissenschaft sowie der Öffentlichkeit zur Verfügung stellt. In ähnlicher Weise ist anlässlich der Revision des Epidemiengesetzes (EpG) angedacht, die im Rahmen des EpG gesammelten und generierten Daten nutzbar zu machen.⁷⁵ Dazu sollen sie in anonymisierter Form der Öffentlichkeit und zu Forschungszwecken zugänglich gemacht werden (Art. 59 Abs. 5 VE-EpG).⁷⁶ Im Einklang mit der OGD-Strategie des Bundes ist zu erwarten, dass in weiteren Bereichen ähnliche Regelungen folgen werden.

2.4. Gentechnik

Das Gentechnikrecht regelt den Umgang mit gentechnisch veränderten Tieren, Pflanzen und anderen Organismen sowie Erzeugnissen, die aus solchen Organismen gewonnen sind (Art. 3 Gentechnikgesetz, GTG). Forschung, Entwicklung sowie Produktion unterliegen, wenn sie in geschlossenen

⁷⁵ Eidgenössisches Departement des Innern (EDI), Teilrevision des Epidemiengesetzes, Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens vom 29. November 2023, 33.

⁷⁶ EDI, Fn. 75, 33. Die Vernehmlassung zum Vorentwurf ist abgeschlossen, siehe zum aktuellen Stand: https://www.fedlex.admin.ch/de/consultation-procedures/ended/2023#https://fedlex.data.admin.ch/eli/dl/proj/2023/5/cons_1 (zuletzt besucht am 27. Mai 2024).

Systemen stattfinden, der Einschliessungsverordnung (ESV).⁷⁷ Führen die Forschungen und Versuche zur Produktreife, gelten, je nach Art des Produkts, unterschiedliche sektorale Regelungen. Handelt es sich um Organismen, die als Produkte dazu bestimmt sind, in der Umwelt freigesetzt zu werden, gelten die Regelungen der Freisetzungsverordnung (FrSV; z.B. beim Saatgut)⁷⁸. Arznei- und Lebensmittel unterliegen dem Produktrecht.⁷⁹

Der Bereich der Gentechnik ist hochreguliert. Die Regulierung erfasst aber nur den Umgang mit gentechnisch veränderten Organismen, d.h. den «zellulären und nichtzellulären biologische Einheiten» (Art. 5 Abs. 1 GTG), nicht den Umgang mit diesbezüglichen Daten. Soweit ersichtlich bestehen keine gesetzlichen Schranken, die einer Veröffentlichung von Gentechnikdaten als ORD entgegenstehen.

2.5. Umweltrecht

Das Umweltrecht umfasst neben dem Umweltschutzgesetz (USG)⁸⁰ und den dazugehörigen Verordnungen auch eine Reihe weiterer Erlasse u.a. in den Bereichen Abfall, Altlasten, Biodiversität, Biotechnologie, Boden, Elektromog, Klima, Landschaft, Lärm, Luft, Naturgefahren, Wald und Holz sowie Wasser.⁸¹

Wegen der unmittelbaren Betroffenheit einer Vielzahl von Personen findet im Umweltrecht weitgehend das **Publizitätsprinzip** Anwendung.⁸² Die Regelungen sehen zum Teil gar vor, dass Daten der Öffentlichkeit zugänglich gemacht werden müssen. Nach Art. 10d Abs. 1 USG können Bericht und Ergebnisse einer Umweltverträglichkeitsprüfung von jedermann eingesehen werden, soweit nicht überwiegende private oder öffentliche Interessen die Geheimhaltung erfordern. Das Fabrikations- und Geschäftsgeheimnis bleibt dabei gemäss Art. 10d Abs. 2 USG auf jeden Fall gewahrt. Diese Pflicht obliegt indes der veröffentlichenden Behörde. Ist die Umweltverträglichkeitsprüfung einmal veröffentlicht, sieht das USG keine Einschränkungen für das weitere Zugänglichmachen der Ergebnisse, etwa als ORD, vor.

⁷⁷ Verordnung über den Umgang mit Organismen in geschlossenen Systemen, SR 814.912.

⁷⁸ Verordnung über den Umgang mit Organismen in der Umwelt, SR 814.911.

⁷⁹ Arzneimittel: Bundesgesetz über Arzneimittel und Medizinprodukte (Heilmittelgesetz, HMG), SR 812.21; Lebensmittel: Bundesgesetz über Lebensmittel und Gebrauchsgegenstände (Lebensmittelgesetz, LMG), SR 817.0.

⁸⁰ SR 814.01.

⁸¹ <<https://www.bafu.admin.ch/bafu/de/home/themen/recht/geltendes-umweltrecht.html>> (zuletzt besucht am 27. Mai 2024).

⁸² THOMAS JUTZI, Unternehmenspublizität, Bern 2017, 48; ROLF H. WEBER, Datenschutz v. Öffentlichkeitsprinzip: Erläuterungen zu den Spannungsfeldern am Beispiel des Zürcher Informations- und Datenschutzgesetzes, Zürich 2010, N 173.

Nach Art. 10e Abs. 1 USG informieren die Behörden die Öffentlichkeit sachgerecht über den Umweltschutz und den Stand der Umweltbelastung. Bei diesen Umweltinformationen handelt es sich um Informationen aus den Regelungsbereichen des USG oder aus dem Bereich der (eidgenössischen oder kantonalen) Gesetzgebung über den Natur- und Heimatschutz, den Landschaftsschutz, den Gewässerschutz, den Schutz vor Naturgefahren, die Walderhaltung, die Jagd und Fischerei, die Gentechnik sowie den Klimaschutz (Art. 7 Abs. 8 USG). Diese Umweltinformationen sind, wenn möglich, als offene digitale Datensätze zur Verfügung zu stellen (Art. 10e Abs. 4 USG).

Auch **Geobasisdaten** sind nach Art. 10 Geoinformationsgesetz (GeoIG)⁸³ grundsätzlich öffentlich zugänglich und können von jeder Person genutzt werden, sofern keine überwiegenden öffentlichen oder privaten Interessen entgegenstehen. Einzelheiten sind in der Geoinformationsverordnung (GeoIV)⁸⁴ geregelt. Diese sieht auch gewisse Einschränkungen bei der Veröffentlichung von Geobasisdaten vor und weist Geobasisdaten drei Zugangsberechtigungsstufen von A – C zu. Die Zugangsberechtigungsstufen der Geobasisdaten können Anhang 1 GeoIV entnommen werden. Zu Geobasisdaten der Stufe A wird der Zugang grundsätzlich gewährt. In Ausnahmefällen kann er aber eingeschränkt, aufgeschoben oder verweigert werden (Art. 22 Abs. 2 GeoIV), etwa wenn Gründe der inneren Sicherheit einer Veröffentlichung entgegenstehen. Zu Geobasisdaten der Zugangsberechtigungsstufe B wird grundsätzlich kein Zugang gewährt (Art. 23 Abs. 1 GeoIV). Von diesem Grundsatz bestehen Ausnahmen, wenn der Zugang den Geheimhaltungsinteressen nicht widerspricht oder die Geheimhaltungsinteressen durch rechtliche, organisatorische oder technische Massnahmen gewahrt werden können (Art. 23 Abs. 2 GeoIV). Zu Geobasisdaten der Zugangsberechtigungsstufe C wird kein Zugang gewährt; davon sind keine Ausnahmen vorgesehen (Art. 24 GeoIV). Nach Art. 25 GeoIV kann eine Einwilligung zur Nutzung von Geobasisdaten zum Eigengebrauch oder zur gewerblichen Nutzung erteilt werden. Die Einwilligung zum Eigengebrauch ermächtigt die Berechtigten aber nicht, die Geobasisdaten als ORD zugänglich zu machen, zumal die Einwilligung nur für die Nutzung zum Eigengebrauch durch eine bestimmte Person und nur gegen Bezahlung einer Gebühr erteilt wird. Da zu Geobasisdaten der Stufe A ohnehin Zugang gewährt wird (Art. 22 Abs. 1 GeoIV), wird man diese aber auch als ORD zugänglich machen dürfen, wenn keine Ausnahme im Sinn von Art. 22 Abs. 2 GeoIV vorliegt.

Damit ist im Ergebnis festzuhalten, dass Forschungsdaten, die Umweltinformationen enthalten, grundsätzlich als ORD veröffentlicht werden können, wenn nicht ausnahmsweise eine Einschränkung vorliegt.

⁸³ Bundesgesetz über Geoinformation, SR 510.62.

⁸⁴ Verordnung über Geoinformation, SR 510.620.

2.6. Chemikalienrecht

Das Chemikaliengesetz (ChemG)⁸⁵, die Chemikalienverordnung (ChemV)⁸⁶, die Biozidprodukteverordnung (VBP)⁸⁷ und die Pflanzenschutzmittelverordnung (PSMV)⁸⁸ enthalten keine Regelungen, die der Veröffentlichung von Forschungsdaten aus diesem Bereich als ORD entgegenstehen.

Die Pflanzenschutzmittelverordnung (PSMV) sieht allerdings einen Berichtschutz für Versuchs- und Studienberichte vor (Art. 46 PSMV). Dieser Schutz steht einem Zugänglichmachen als ORD zwar nicht per se entgegen. Allerdings dürfen geschützte Berichte durch die Zulassungsstelle grundsätzlich nicht zum Nutzen einer anderen Gesuchstellerin für Bewilligungen für Pflanzenschutzmittel, Safener oder Synergisten und Zusatzstoffe verwendet werden (Art. 46 Abs. 3 PSMV). Der Berichtschutz gilt für einen Zeitraum von zehn Jahren (Art. 46 Abs. 4 PSMV).

Das BAG kann Dritten ferner Daten aus der Radondatenbank zu Forschungszwecken zur Verfügung stellen. Dies ist allerdings u.a. mit der Auflage verbunden, dass die Daten nicht weitergegeben werden (Art. 162 Abs. 5 lit. b Strahlenschutzverordnung). Entsprechende Daten dürfen also nicht als ORD zugänglich gemacht werden.

2.7. Lebensmittelrecht

Die rechtlichen Grundlagen für Daten aus dem Lebensmittelbereich sind primär das Lebensmittelgesetz (LMG)⁸⁹ und die Verordnung über den Vollzug der Lebensmittelgesetzgebung (LMVV)⁹⁰. Art. 40 Abs. 1 LMG sieht vor, dass der Bund die für die Anwendung des LMG erforderlichen wissenschaftlichen Grundlagen erforscht und beschafft. Er kann diese Erhebungen selbst oder in Zusammenarbeit mit den Kantonen durchführen (Art. 40 Abs. 2 LMG). Ist dies der Fall, so dürfen Ergebnisse von Forschungsarbeiten und Erhebungen der Öffentlichkeit nicht zugänglich gemacht werden, soweit diese Rückschlüsse auf betroffene Herstellerinnen, Vertreiberinnen oder Produkte zulassen (Art. 24 Abs. 4 lit. b LMG). Es ist denkbar, dass die Institutionen des ETH-Bereichs gestützt auf Art. 40 LMG Forschung betreiben, was einer Veröffentlichung von Forschungsdaten aus dem Lebensmittelbereich als ORD entgegenstehen könnte. Darüber hinaus finden sich in den rechtlichen Grundlagen keine (weiteren) Schranken, die einem Zugänglichmachen von Forschungsdaten als ORD entgegenstehen.

⁸⁵ Bundesgesetz über den Schutz vor gefährlichen Stoffen und Zubereitungen, SR 813.1.

⁸⁶ Verordnung über den Schutz vor gefährlichen Stoffen und Zubereitungen, SR 813.11.

⁸⁷ Verordnung über das Inverkehrbringen von und den Umgang mit Biozidprodukten, SR 813.12.

⁸⁸ Verordnung über das Inverkehrbringen von Pflanzenschutzmitteln, SR 916.161.

⁸⁹ Bundesgesetz über Lebensmittel und Gebrauchsgegenstände, SR 817.0.

⁹⁰ SR 817.042.

2.8. Energie- und Kernenergierecht

Im Energierecht bestehen Schranken für die Veröffentlichung von Forschungsdaten zum Schutz von kritischen Infrastrukturen. Kritische Infrastrukturen sind Prozesse, Systeme und Einrichtungen, die für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung essenziell sind. Für die Schweiz umfasst das Spektrum der kritischen Infrastrukturen im Energierecht die Bereiche Erdgasversorgung, Erdölversorgung, Stromversorgung, Wasserversorgung, Fern- und Prozesswärme, Abfälle und Abwasser.⁹¹ Das Inventar kritischer Infrastrukturen (SKI-Inventar) definiert Bauten und Anlagen, die entweder aus nationaler oder aus kantonaler Perspektive eine strategisch wichtige Bedeutung haben. Es ist in seiner Gesamtheit als geheim klassifiziert. Auszüge, die nur einen Teil der Informationen enthalten (z.B. aus einem Kanton oder einem Sektor) sind in der Regel als vertraulich klassifiziert.⁹² Betreffen Forschungsdaten Informationen über kritische Infrastrukturen, dürfen sie nicht als ORD öffentlich zugänglich gemacht werden.

Im Bereich der **Kernenergie** besteht ein öffentliches Geheimhaltungsinteresse hinsichtlich diverser Belange, bspw. rund um die Nutzung radioaktiver Elemente und den Betrieb von Kernkraftwerken, um die Sicherheit und den Schutz vor Sabotageakten oder Terroranschlägen zu gewährleisten. Art. 91 Abs. 1 lit. b Kernenergiegesetz (KEG)⁹³ stellt Geheimnisverletzung unter Strafe. Strafbar macht sich demnach, wer geheime Tatsachen oder Vorkehren, die dem Schutz von Kernanlagen, Kernmaterialien oder radioaktiven Abfälle vor Einwirkungen Dritter oder vor kriegesischen Einwirkungen dienen, unbefugt bekannt oder zugänglich macht.

Welche Informationen von der Strafbestimmung bei Geheimnisverletzung in Art. 91 Abs. 1 lit. b KEG umfasst sind, lässt sich nicht abstrakt festlegen. Bei der Verwendung von Forschungsdaten im Zusammenhang mit der Kernenergie muss deshalb beachtet werden, dass diese nur dann als ORD zugänglich gemacht werden, wenn sie nach Art. 74 Abs. 1 KEG der Öffentlichkeit zugänglich gemacht werden können und es sich nicht um geheime Tatsachen und Vorkehren handelt, die dem Schutz von Kernanlagen, Kernmaterialien oder radioaktiven Abfälle vor Einwirkungen Dritter oder vor kriegesischen Einwirkungen dienen. Wer solche Forschungsdaten als ORD zugänglich macht, macht sich nach Art. 91 Abs. 1 lit. b KEG strafbar.

⁹¹ BUNDESAMT FÜR BEVÖLKERUNGSSCHUTZ, Nationale Strategie zum Schutz kritischer Infrastrukturen, Ganzheitlicher Ansatz zur Sicherstellung der Verfügbarkeit von essenziellen Gütern und Dienstleistungen vom 16. Juni 2023, BBl 2023 1659, 7 f.

⁹² <<https://www.babs.admin.ch/de/die-kritischen-infrastrukturen>> (zuletzt besucht am 27. Mai 2024).

⁹³ SR 732.1.

Eine weitere Hürde für ORD im Zusammenhang mit Daten aus der Kernenergie ist in Art. 13 Kernenergieverordnung (KEV)⁹⁴ zu finden. Art. 13 KEV sieht eine Bewilligungspflicht für die Ausfuhr und Vermittlung von Technologie vor, die Kernmaterialien betrifft. Technologie in diesem Zusammenhang meint spezifisches, allgemein nicht zugängliches oder nicht der wissenschaftlichen Grundlagenforschung dienendes Wissen in Form von technischen Daten oder technische Unterstützung, die für die Entwicklung, Herstellung oder Verwendung von Kernmaterialien erforderlich ist. Sollen also Forschungsdaten mit solchen Informationen als ORD zugänglich gemacht werden, bedarf dies einer Bewilligung. Die Bewilligung zur Ausfuhr und Vermittlung wird erteilt, wenn die Bewilligungsvoraussetzungen nach Art. 7 lit. a f. KEV eingehalten sind. Namentlich müssen der Schutz von Mensch und Umwelt und die nukleare Sicherheit und Sicherung gewährleistet sein und es dürfen keine Gründe der Nichtverbreitung von Kernwaffen, die von der Schweiz unterstützt werden, entgegenstehen. Wann Technologien betreffend Kernmaterialien die Ausfuhr- und Vermittlungsbewilligungen einhalten, muss im Einzelfall geprüft werden. Ohne eine solche Bewilligung für die Ausfuhr und Vermittlung können diese Forschungsdaten nicht als ORD zugänglich gemacht werden.

Im Energie- und Kernenergierecht bestehen rechtliche Schranken, die einer Veröffentlichung von bestimmten Forschungsdaten als ORD entgegenstehen. Im Energierecht betreffen die Schranken Daten zum Inventar kritischer Infrastruktur, die geheim bzw. vertraulich zu behandeln ist. Im Bereich der Kernenergie bestehen Schranken für Informationen, die dem Schutz von Kernanlagen, Kernmaterialien oder radioaktiven Abfällen vor Einwirkungen Dritter oder vor kriegesischen Einwirkungen dienen und für Daten, deren Ausfuhr oder Vermittlung eine Gefahr für die nukleare Sicherheit schaffen würde.

2.9. Tierschutzrecht

Im Tierschutzrecht sind in erster Linie das Tierschutzgesetz (TSchG)⁹⁵ und die Tierschutzverordnung (TSchV)⁹⁶ zu beachten, die den Schutz von Wirbeltieren (also Säugetieren, Fischen, Vögel, Amphibien und Reptilien) regeln. Wirbellose Tiere (bspw. Schnecken, Spinnen, Würmer etc.) sind vom Anwendungsbereich ausgenommen. Neben dem Tierschutz- bzw. Tierwohlrecht betreffen eine Reihe weiterer Rechtsgebiete Tiere, etwa in der Tierzucht, im Veterinärrecht, bei den landwirtschaftlichen Direktzahlungen, beim Artenschutz, Jagd- und Fischereirecht oder im Lebensmittelrecht.

Die Analyse der einschlägigen gesetzlichen Grundlagen im Tierschutzrecht zeigt, dass einer Veröffentlichung von Forschungsdaten als ORD keine gesetzlichen Schranken entgegenstehen.

⁹⁴ SR 732.11.

⁹⁵ SR 45.

⁹⁶ SR 455.1.

2.10. Finanzmarktrecht

Im Bereich des Finanzmarktrechts ist namentlich die Einhaltung des Bankgeheimnisses zu beachten. Der Geheimhaltungspflicht nach Art. 47 Bankengesetz (BankG)⁹⁷ unterliegen alle Kenntnisse, die sich aus der geschäftlichen Beziehung der Bank zum Kunden, namentlich aus Bankverträgen ergeben, darüber hinaus aber auch Anfragen und Angebote für weitere Bankgeschäfte und der Geschäftsverkehr unter Banken.⁹⁸

Die Geheimhaltungspflicht erfasst alle in einer Bank oder für sie vertraglich tätigen Personen. Wissenschaftlich arbeitenden Personen darf eine Bank nur Zugang zu den Kundendaten gewähren, wenn mit ihnen ein Arbeits- oder Auftragsverhältnis besteht (Art. 47 Abs. 1 BankG). Zwingend bleibt in jedem Fall die Anonymisierung der Kundendaten in einer allfälligen Publikation, soweit Kunden der Offenlegung nicht ausdrücklich zustimmen.⁹⁹ Anonymisierte Bankdaten sind keine Personendaten mehr, wenn nach dem gewöhnlichen Lauf der Dinge kein Betroffener die Mittel einsetzen kann, die vernünftigerweise für die Re-Identifizierung verwendet werden können. Bankdaten werden dem Schutz des Bankgeheimnisses entzogen, wenn sie anonymisiert sind.¹⁰⁰ Wurden Bankdaten in anonymisierter Form an Forschende übermittelt, kann in der Regel davon ausgegangen werden, dass die Publikation dieser Daten als ORD das Bankgeheimnis nicht verletzt und damit zulässig ist. Daten, die dem Bankgeheimnis unterstehen, können folglich nur anonymisiert als ORD zugänglich gemacht werden.

Im Ergebnis kann festgehalten werden, dass Forschungsdaten, die dem Bankgeheimnis unterstehen, nicht als ORD zugänglich gemacht werden dürfen. Sind die Bankkundendaten anonymisiert, kann eine Publikation als ORD erfolgen.

Aus den Regelungen der Finanzdienstleistungen¹⁰¹ und Finanzinstitute¹⁰² ergeben sich keine rechtlichen Schranken für ORD.

⁹⁷ Bundesgesetz über die Banken und Sparkassen, SR 952.0.

⁹⁸ BEAT KLEINER/RENATE SCHWOB/CHRISTOPH WINZELER, Kommentar zum Bundesgesetz über die Banken und Sparkassen vom 8. November 1934 sowie zu der Verordnung vom 17. Mai 1972 (V) und der Vollziehungsverordnung (VV) vom 30. August 1961 (VV) – mit Hinweisen auf das Bankenrecht der Europäischen Union, auf das Allgemeine Dienstleistungsabkommen (GATS) und mit Erläuterungen zu den Massnahmen gegen die Geldwäscherei, Zobl/Schwob/Winzeler/Kaufmann/Weber/Kramer (Hrsg.), Zürich 2015, Art. 47 N 8 f.

⁹⁹ BankG-Komm., KLEINER/SCHWOB/WINZELER, Fn. 98, Art. 47 N 335, 360.

¹⁰⁰ CÉLIAN HIRSCH/ÉMILIE JACOT-GUILLARMOD, Les données bancaires pseudonymisées – Du secret bancaire à la protection des données, SZW 2020, 151 ff., 156.

¹⁰¹ Bundesgesetz über die Finanzdienstleistungen (Finanzdienstleistungsgesetz, FIDLEG), SR 950.1.

¹⁰² Bundesgesetz über die Finanzinstitute (Finanzinstitutsgesetz, FINIG), SR 954.1.

3. Rechte Dritter

Dem Zugänglichmachen von Forschungsdaten können nicht nur gesetzliche Vorgaben, sondern auch Rechte Dritter entgegenstehen. Im Vordergrund stehen dabei Urheberrechte, Ansprüche aus dem strafrechtlichen Geheimnisschutz (Art. 162 StGB), Ansprüche aus dem UWG (Art. 5 lit. c und Art. 6 UWG) und Ansprüche aus dem Datenschutzrecht. Patente können dem Zugänglichmachen von Forschungsdaten dagegen nicht entgegengehalten werden.

3.1. Urheberrechte

Wir gehen davon aus, dass in der Regel weder Werke der Literatur und Kunst oder geschützten Leistungen noch Computerprogramme ganz oder in Teilen als ORD zugänglich gemacht werden. Vor dem Zugänglichmachen von ORD ist aber stets zu **prüfen, ob die Daten urheberrechtlich geschützte Werke oder Teile davon enthalten**.¹⁰³ Das ist bspw. der Fall, wenn genügend lange Sequenzen von Source Code oder von Texten, Bildern oder Fotografien zugänglich gemacht werden. Trifft dies zu, müssen die Inhaber der Urheberrechte an diesen Werken angefragt werden, ob sie mit dem Zugänglichmachen ihrer Werke einverstanden sind.

Grössere Mengen von Forschungsdaten, die als ORD zugänglich gemacht werden, werden regelmässig als Datenbanken im Sinn des Urheberrechts zu qualifizieren sein. Wenn es sich um **strukturierte Datenbanken** handelt, können diese urheberrechtlich geschützt sein. Vor dem Zugänglichmachen von Daten als ORD ist deshalb stets zu prüfen, ob die Daten als Datenbank zu qualifizieren sind, die urheberrechtlich geschützt sein könnte. Ist dies der Fall, müssen die Rechteinhaber angefragt werden, ob sie mit dem Zugänglichmachen der Datenbank einverstanden sind.

Die Urheberrechte gehören den Personen, welche die Datenbank erstellt haben (Art. 6 URG). Soweit es sich um Datenbanken handelt, die von Mitarbeitenden einer Institution des ETH-Bereichs erstellt wurden, gehören die Urheberrechte an den Datenbanken diesen Mitarbeitenden (Art. 36 Abs. 1 ETH-Gesetz). Diese Regelung erscheint zwar wenig sinnvoll, zumal die Urheberrechte an Source Code von Gesetzes wegen an die Institutionen des ETH-Bereichs übertragen werden (Art. 36 Abs. 2 ETH-Gesetz), sie ergibt sich aber unzweideutig aus der Regelung in Art. 36 Abs. 1 und Abs. 2 ETH-Gesetz. Die Mitarbeitenden können damit selbst entscheiden, ob sie Datenbanken als ORD zugänglich machen wollen, soweit die jeweilige Institution des ETH-Bereichs keine interne Regelung erlassen hat, die einen Übergang der Urheberrechte an Datenbanken an die Institution oder ein Zugänglichmachen von Forschungsdaten (und/oder Datenbanken) als ORD vorschreibt. Wurde eine **Datenbank von Dritten erstellt, sind diese anzufragen**. Dabei ist stets zu prüfen, ob die Urheber der Datenbank ihre Rechte an

¹⁰³ Siehe dazu vorne, B.1.2.

andere Dritte abgetreten haben, bspw. an eine Hochschule, einen Verlag oder einen kommerziellen Anbieter. Trifft dies zu, muss deren Zustimmung eingeholt werden.

3.2. Patente

Patente werden für **Erfindungen** erteilt, also für **Lehren zum technischen Handeln**.¹⁰⁴ Sie verschaffen ihrem Inhaber das Recht, anderen zu verbieten, die Erfindung gewerbmässig zu benutzen (Art. 8 Abs. 1 PatG). Als Benützung gelten dabei insb. das Herstellen, das Lagern, das Anbieten, das Inverkehrbringen, die Ein-, Aus- und Durchfuhr sowie der Besitz zu diesen Zwecken (Art. 8 Abs. 2 PatG). Bei der Benützung ist zwischen **Erzeugnis- und Verfahrenspatenten** zu unterscheiden. Als Benützung gelten bei Erzeugnispatenten die Herstellung und Kommerzialisierung der patentierten Erfindung. Erfasst werden damit alle (aber nur) Handlungen, die das patentgeschützte Erzeugnis betreffen, diese umfassen neben dem Herstellen auch das Lagern, Anbieten, Inverkehrbringen (etc.) eines solchen Erzeugnisses. Bei Verfahrenspatenten liegt eine Benützung vor, wenn das Verfahren angewendet wird, wenn also die in den Patentansprüchen vorgesehenen Verfahrensschritte durchgeführt werden.

Als ORD zugänglich gemachte Forschungsdaten können patentierte Erfindungen enthalten. Das dürfte zwar selten vorkommen, kann aber nicht ausgeschlossen werden. Das Zugänglichmachen einer Erfindung über das Internet ist aber **keine Benützung einer Erfindung** im Sinn des Patentrechts, weil dadurch weder ein Erzeugnis hergestellt noch ein Verfahren ausgeführt wird. Das Zugänglichmachen kann deshalb vom Patentinhaber nicht verboten werden.

Zu beachten ist zudem, dass Patente nur erteilt werden, wenn die **Erfindung in der Patentanmeldung offenbart** wird. Das bedeutet, dass die Erfindung in der Patentanmeldung so deutlich und vollständig dargelegt werden muss, dass sie eine Fachperson aufgrund der Patentschrift und unter Einbezug des allgemeinen Fachwissens auf dem betreffenden Fachgebiet ausführen kann (Art. 50 Abs. 1 PatG).¹⁰⁵ Da die Patentschrift mit der Erteilung des Patents auf der Website des Patentamtes veröffentlicht wird, ist die Erfindung mit Erteilung des Patents ohnehin öffentlich zugänglich. Sollten als ORD zugänglich gemachte Forschungsdaten eine patentierte Erfindung enthalten, würde damit keine Information offenbart, die nicht ohnehin schon öffentlich zugänglich ist.

¹⁰⁴ MARK SCHWEIZER/HERBERT ZECH, in: Schweizer/Zech (Hrsg.), Stämpfli Handkommentar, Patentgesetz (PatG), Bundesgesetz über die Erfindungspatente vom 25. Juni 1954, Bern 2019, Art. 1 N 10; BGer 4A.12/1995 vom 31. Juli 1996, E. 4, in: sic! 1997, 77 ff.: In seiner Entscheidung definierte das Bundesgericht eine technische Erfindung als «Lehre zum planmässigen Handeln unter Einsatz beherrschbarer Naturkräfte zur unmittelbaren Erreichung eines kausal übersehbaren Erfolgs».

¹⁰⁵ HGer SG, sic! 2009, 875 ff., 879 ff. – «Dichtmasse»; SHK PatG-SUTTER/HOCHREUTENER, Fn. 104, Art. 50 N 3 f.

3.3. Ansprüche aus dem strafrechtlichen Geheimnisschutz

Werden Forschungsdaten als ORD zugänglich gemacht, obwohl die Forschenden und/oder die Institution des ETH-Bereichs gesetzlich oder vertraglich zur Geheimhaltung verpflichtet sind, liegt ein Verstoß gegen Art. 162 StGB vor. Die natürliche Person, welche die Daten zugänglich gemacht hat, kann auf Antrag des Geheimnisherrn mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft werden (Art. 162 StGB).

Zum Stellen des Strafantrags ist der **Geheimnisherr** berechtigt. Geheimnisherr wird in der Regel eine andere Forschungsinstitution oder ein Unternehmen sein, die einem Forschenden oder einer Institution des ETH-Bereichs Forschungsdaten zugänglich gemacht hat und die Forschenden oder die Institution zur Geheimhaltung verpflichtet hat. Der Geheimnisherr kann nicht nur Antrag auf Strafe stellen, sondern auch Unterlassung der Verletzung und Schadenersatz verlangen. Der Anspruch auf Schadenersatz ergibt sich aus dem allgemeinen Deliktsrecht (Art. 41 OR i.V.m. Art. 162 StGB). Der Anspruch auf Unterlassung ist zwar nicht ausdrücklich vorgesehen, lässt sich aber aus dem allgemeinen Deliktsrecht (Art. 41 ff. OR) ableiten. Denn dieses vermittelt nicht nur einen Anspruch auf Schadenersatz, sondern richtigerweise auch einen Anspruch auf Unterlassung.¹⁰⁶

3.4. Ansprüche aus UWG

Das UWG ist auf alle Handlungen anwendbar, die auf die Beeinflussung des Wettbewerbs auf einem (bestimmten) Markt angelegt sind. Erfasst werden damit alle Handlungen, die **marktrelevant, marktgeneigt oder wettbewerbsgerichtet** sind und die sich auf das Verhältnis zwischen Mitbewerbern oder auf das Verhältnis zwischen Anbietern und Abnehmern auswirken können. Auf die wissenschaftliche Forschung und die Publikation ihrer Ergebnisse ist das UWG dagegen nicht anwendbar, solange diese Tätigkeiten im akademischen Rahmen erfolgen.¹⁰⁷ Auf Kooperationen mit privaten Unternehmen und wenn die Forschungsergebnisse (z.B. von einem Start-up) am Markt verwertet werden sollen, findet das UWG aber Anwendung.

Das Übernehmen und Zugänglichmachen von Forschungsdaten als ORD kann gegen das **Verbot der unmittelbaren Übernahme (Art. 5 lit. c UWG)** verstossen oder als **Verletzung von Fabrikations- und Geschäftsgeheimnissen (Art. 6 UWG)** zu qualifizieren sein. Letzteres ist allerdings nur der Fall, wenn ein Verletzer die Daten ausgekundschaftet oder sonst wie unrechtmässig erfahren hat.¹⁰⁸

¹⁰⁶ MARTIN A. KESSLER, in: Widmer Lüchinger/Oser (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR, Basel 2020, Art. 43 N 4; in diese Richtung auch MARTIN ECKERT, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 2016, 245 ff., 272 und URS HESS-ODONI, Die Herrschaftsrechte an Daten, in: Jusletter vom 17. Mai 2004, Rz. 39.

¹⁰⁷ BGer 6B_188/2013 vom 4. Juli 2013, E. 6.3, m.w.H.

¹⁰⁸ Siehe dazu vorne, B.1.5.

Wer durch den Verstoss gegen eine Bestimmung des UWG in seiner Kundschaft, seinem Kredit oder beruflichen Ansehen, in seinem Geschäftsbetrieb oder sonst in seinen wirtschaftlichen Interessen bedroht oder verletzt wird, kann Unterlassung der Verletzung, Beseitigung der Folgen der Verletzung und Schadenersatz sowie Herausgabe des Gewinns verlangen (Art. 9 UWG). Ein Verstoss gegen Art. 5 lit. c oder Art. 6 UWG ist zudem strafbar; der Täter wird auf Antrag mit bis zu drei Jahren Gefängnis oder Geldstrafe bestraft (Art. 23 UWG). Zur Klage auf Unterlassung, Beseitigung und Schadenersatz bzw. Gewinnherausgabe und zum Stellen eines Strafantrags ist der *«data owner»* berechtigt, also der **Inhaber der faktischen Herrschaft über die Daten**, die durch Art. 5 lit. c und Art. 6 UWG rechtlich abgesichert ist.

3.5. Datenschutzrechtliche Ansprüche

Das Datenschutzrecht vermittelt den betroffenen Personen **kein umfassendes Herrschaftsrecht** an den sie betreffenden Daten, aber bestimmte Ansprüche, mit denen sie die Nutzung der Daten bis zu einem gewissen Grad kontrollieren und beschränken können. Diese Möglichkeiten gehen wesentlich weiter, wenn die Daten von einer privaten Person, insb. von einem Unternehmen, bearbeitet werden. Die Bearbeitung durch Unternehmen beruht in gewissen Fällen auf der Einwilligung der betroffenen Personen, die jederzeit widerrufen werden kann.¹⁰⁹ Zudem können die betroffenen Personen Widerspruch gegen die Bearbeitung der sie betreffenden Daten erheben (Art. 30 Abs. 2 lit. b DSG). Beides hat zur Folge, dass die Daten von der privaten Person nur noch bearbeitet werden dürfen, wenn sie ein überwiegendes Interesse an der Bearbeitung hat (Art. 31 DSG).

Die Bearbeitung von Personendaten durch Bundesorgane beruht immer auf einer **gesetzlichen Grundlage**. Eine Einwilligung der betroffenen Personen ist für diese Bearbeitung nicht erforderlich. Das gilt auch für die Bearbeitung von Personendaten für die Forschung durch die Institutionen des ETH-Bereichs. An dieser Rechtslage ändert nichts, dass die betroffenen Personen regelmässig ihre Einwilligung in die Bearbeitung von Personendaten für die Forschung erteilen. Das **Einholen einer Einwilligung** ist (forschungs-)ethisch zweifellos zu begrüssen, in zahlreichen Standards vorgesehen und in vielen Bereichen etablierte Praxis, aber **datenschutzrechtlich nicht erforderlich**. Weder für die Bearbeitung im Rahmen eines Forschungsprojekts noch für das Zugänglichmachen der Forschungsdaten als ORD in anonymisierter Form. Da die Bearbeitung von Personendaten für die Forschung an den Institutionen des ETH-Bereichs rechtlich nicht auf einer Einwilligung beruht, können die betroffenen Personen die Bearbeitung der sie betreffenden Daten auch nicht durch Entzug der Einwilligung oder durch Ausüben eines Widerspruchs- oder Löschungsrechts rechtswirksam verhindern. Die

¹⁰⁹ BSK DSG-BÜHLMANN/REINLE, Fn. 59, Art. 6 N 316; SHK DSG-BAERISWYL, Fn. 59, Art. 6 N 84.

betroffenen Personen haben damit keine Rechte, die es ihnen ermöglichen, das Zugänglichmachen von sie betreffenden «Personendaten» als ORD zu verhindern.

Wie vorstehend ausgeführt, dürfen Personendaten schon aufgrund der allgemeinen datenschutzrechtlichen Vorgaben **nur in anonymisierter Form als ORD zugänglich** gemacht werden.¹¹⁰ Ist diese Voraussetzung erfüllt, dann ist das DSG auf das Zugänglichmachen der Daten gar nicht anwendbar. Den betroffenen Personen stehen schon deshalb keine datenschutzrechtlichen Ansprüche zu, die sie gegen das Zugänglichmachen von Forschungsdaten als ORD geltend machen könnten.

4. Vertragliche Schranken

Forschungsvorhaben werden oft im Rahmen einer Zusammenarbeit mehrerer Hochschulen und/oder in Zusammenarbeit mit Unternehmen umgesetzt. Diese Kooperationen werden in der Regel in Verträgen geregelt, die regelmässig Vereinbarungen über die Geheimhaltung der Forschungsergebnisse enthalten. Aus diesen **Geheimhaltungsverpflichtungen** können sich Schranken für ORD ergeben. Diese Verpflichtungen können insb. in Kooperations- oder Lizenzverträgen, in «Non Disclosure Agreements» (NDA) oder in «Material Transfer Agreements» (MTA) vorgesehen sein. Schranken für ORD können sich aber auch aus **anderen vertraglichen Vereinbarungen** ergeben, die den Umgang mit Forschungsdaten regeln.

Solche vertraglichen Vorgaben können im **Widerspruch zur ORD-Strategie** einer Institution des ETH-Bereichs oder zu deren konkreten Umsetzung in Gesetzen oder internen Richtlinien stehen. In diesem Fall stellt sich die Frage, ob die vertragliche Vereinbarung gültig ist. Für die inhaltliche Ausgestaltung von Verträgen besteht Vertragsfreiheit. Schranken können sich aber aus Art. 19 Abs. 2 OR ergeben, wonach eine vertragliche Vereinbarung nicht gegen zwingende Vorgaben des Gesetzes, gegen die guten Sitten oder die öffentliche Ordnung verstossen darf. Auch Verträge mit unmöglichem, widerrechtlichem oder unsittlichem Inhalt sind nichtig (Art. 20 Abs. 2 OR). Unzulässig sind zudem Verträge, die eine Partei übermässig binden (Art. 27 Abs. 2 ZGB). Je nach Ausgestaltung können Vorgaben zu ORD als zwingendes Recht zu qualifizieren sein. Ein Vertrag ist **widerrechtlich** i.S.v. Art. 19/20 OR, wenn sein Inhalt einer zwingenden objektiven, privat- oder öffentlich-rechtlichen Norm des – geschriebenen oder ungeschriebenen – schweizerischen (eidgenössischen oder kantonalen) Rechts widerspricht.¹¹¹ Ob eine Norm zwingend ist, ergibt sich aus der Auslegung der entsprechenden Norm.¹¹²

¹¹⁰ Siehe dazu vorne, 0.

¹¹¹ BSK OR I-MEISE/HUGUENIN, Fn. 106, Art. 19/20 N 15; AHMET KUT/CHRISTOPH BAUER, in: Atamer/Furrer (Hrsg.), Handkommentar zum Schweizer Privatrecht, Obligationenrecht – Allgemeine Bestimmungen – Art. 1-183 OR, Zürich 2023, Art. 20 N 13; BGer 4A_173/2010 vom 22. Juni 2010, E. 2.2.

¹¹² BSK OR I-MEISE/HUGUENIN, Fn. 106, Art. 19/20 N 20 f.; CHK OR-KUT/BAUER, Fn. 111, Art. 20 N 14; BGE 143 III 600, E. 2.8.1.

Wenn ein Vertrag zwischen Forschenden und einem Vertragspartner eine Vereinbarung enthält, die nicht mit der ORD-Strategie der Hochschule im Einklang steht, ist eine zweistufige Prüfung vorzunehmen: In einem ersten Schritt ist zu prüfen, ob es sich bei der potenziell durch den Vertrag verletzten Norm um eine **gesetzliche Vorschrift** im Sinne von Art. 19/20 OR handelt. Dies ist bspw. beim ETH-Gesetz der Fall; dieses enthält allerdings keine Vorgaben für ORD. Bei internen Richtlinien ist zu prüfen, ob sie als gesetzliche Vorschriften im Sinn von Art. 19/20 OR zu qualifizieren sind. In einem zweiten Schritt ist zu untersuchen, ob die in Frage stehenden **Vorschrift zwingend** ist. Trifft dies zu, ist der Vertrag nichtig (Art. 20 Abs. 1 OR). Die Nichtigkeitsfolge tritt jedoch nach herrschender Lehre und Praxis nicht automatisch ein, sondern nur, «wenn diese Rechtsfolge vom Gesetz ausdrücklich vorgesehen wird oder sich aus dem Sinn und Zweck der verletzten Norm ergibt».¹¹³ Nach dem Grundsatz der Teilnichtigkeit geht die Nichtigkeit zudem nur soweit, wie es der Schutzzweck der verletzten Norm verlangt.

Der Schutzzweck von Bestimmungen, die ORD betreffen, dürfte in der Regel keine vollständige Nichtigkeit des Vertrages verlangen. Vielmehr dürfte es dem Zweck der betreffenden Bestimmung entsprechen, dass nur diejenigen Bestimmungen des Vertrages als nichtig betrachtet würden, die gegen die ORD-relevante Bestimmung verstossen. Ausnahmen gelten nur, wenn anzunehmen ist, dass der gesamte Vertrag ohne den widerrechtlichen Inhalt nicht geschlossen worden wäre.¹¹⁴ Das könnte bspw. der Fall sein, wenn ein Kooperationsvertrag eine Pflicht zur Geheimhaltung von Forschungsdaten vorsieht, die wegen eines Verstosses gegen eine ORD-Bestimmung nichtig ist, und der Vertragspartner den Vertrag nicht geschlossen hätte, wenn ihm bewusst gewesen wäre, dass die Forschungsdaten als ORD zugänglich gemacht werden müssen.

Auch aus **Lizenzverträgen** können sich Schranken für ORD ergeben. Neben Geheimhaltungsverpflichtungen können Lizenzverträge bspw. gewisse Nutzungsbeschränkungen in geographischer oder zeitlicher Hinsicht enthalten, die ORD entgegenstehen. Auch Vorgaben zur Weitergabe und Publikation von Daten, bspw. die Verpflichtung zur Veröffentlichung von Daten auf einer bestimmten Plattform, können mit ORD-Vorgaben der Institutionen des ETH-Bereichs kollidieren.

5. Verantwortlichkeit

Wenn Forschende die Schranken für ORD missachten und dadurch Dritten ein Schaden entsteht, kommen die allgemeinen Bestimmungen zur Verantwortlichkeit zur Anwendung.

¹¹³ BSK OR I-MEISE/HUGUENIN, Fn. 106, Art. 19/20 N 54, m.w.H.; BGE 143 III 600, E. 2.8.1; BGE 134 III 438, E. 2.2; BGE 123 III 292, E. 2.e.aa.

¹¹⁴ BSK OR I-MEISE/HUGUENIN, Fn. 106, Art. 19/20 N 64a; CHK OR-KUT/BAUER, Fn. 111, Art. 20 N 49; BGer 4C.156/2006 vom 17. August 2006, E. 3.4; BGE 143 III 558, E. 4.1.1; BGE 124 III 57, E. 3.c, m.w.H.

Im **Aussenverhältnis**, also gegenüber Dritten, haften die Institutionen des ETH-Bereichs ohne Rücksicht auf das Verschulden ihrer Angestellten für den Schaden, den ihre Angestellten Dritten in Ausübung ihrer dienstlichen Tätigkeit widerrechtlich zugefügt haben (Art. 3 Abs. 1 i.V.m. Art. 19 Abs. 1 lit. a Verantwortlichkeitsgesetz (VG) i.V.m. Art. 5 Abs. 1 ETH-Gesetz). Für gewisse Rechtsbereiche gelten besondere Vorschriften (bspw. Art. 30 ff. GTG), die dem VG vorgehen (Art. 3 Abs. 2 VG), hier aber kaum relevant sein dürften. Auch Verträge enthalten bisweilen Bestimmungen, welche die Folgen von Vertragsverletzungen regeln, bspw. durch Festlegung von Konventionalstrafen.

Im **Innenverhältnis**, d.h. im Verhältnis zwischen den Angestellten und der Institution des ETH-Bereichs, kommen die jeweiligen internen Richtlinien zur Anwendung, namentlich die Vorschriften über das Zugänglichmachen von Forschungsdaten als ORD sowie Vorschriften über die wissenschaftliche Integrität und Vorgaben zum Vorgehen bei wissenschaftlichen Fehlverhalten.

D. RECHTLICHE UMSETZUNG VON ORD

1. Vorbemerkung

Die Verfassung enthält die grundlegenden staatlichen Normen. Ein wichtiger Teil sind die Grundrechte, welche den Individuen wesentliche Rechte gegenüber dem Staat garantieren. Als Staat gilt nicht nur der Staat selbst, sondern auch, wer staatliche Aufgaben wahrnimmt (Art. 35 Abs. 2 BV). Die **Institutionen des ETH-Bereichs** nehmen staatliche Aufgaben wahr und sind in ihrem Handeln **an die Grundrechte gebunden**. Diese Vorgaben sind auch bei der Umsetzung von ORD zu beachten.

Sofern keine gesetzlichen Schranken bestehen und Dritte keine Rechte an den Forschungsdaten haben oder auf die Ausübung dieser Rechte verzichten, können Forschungsdaten frei als ORD zugänglich gemacht werden. Aus rechtlicher Sicht kann der **Zugriff auf ORD vollkommen frei** erfolgen, also ohne Abschluss eines Lizenzvertrags und ohne Zustimmung zu Nutzungsbedingungen und damit ohne, dass den Nutzenden Restriktionen beim Zugang und bei der Nutzung der Daten auferlegt werden.

In der Regel wird der Betreiber einer ORD-Plattform die Forschungsdaten aber nur auf Grundlage eines **Lizenzvertrags** zur Verfügung stellen, um die Einhaltung gewisser Bedingungen (z.B. Angabe der Quelle oder Einhalten wissenschaftlicher Standards) sicherzustellen. Das Positionspapier des ETH-Rates sieht denn auch vor, dass die Verwendung von ORD auf Grundlage einer Lizenz erfolgen soll.¹¹⁵

¹¹⁵ ETH-RAT, Open Research Data, Position of the ETH Domain, 5.

2. Verfassungsrechtliche Rahmenbedingungen

Die Umsetzung einer ORD-Strategie kann auf verschiedene Weise erfolgen. Um den Ansatz effektiv umzusetzen, kann es notwendig sein, Forschende zu verpflichten, ihre Forschungsdaten öffentlich zugänglich zu machen. Eine solche Verpflichtung kann aus grundrechtlicher Sicht relevant sein. Betroffen sein können die Grundrechte der Wissenschaftsfreiheit, der Eigentumsgarantie und der Wirtschaftsfreiheit.

2.1. Für ORD relevante Grundrechte

Das wichtigste Grundrecht im Zusammenhang mit ORD ist die **Wissenschaftsfreiheit**, welche die wissenschaftliche Lehre und Forschung schützt (Art. 20 BV).¹¹⁶ Betroffen sind die Forschenden, denen durch Vorgaben zu ORD ein bestimmter Umgang mit Forschungsdaten vorgeschrieben wird. Dem steht die Wissenschaftsfreiheit der anderen Forschenden und der Mitglieder der wissenschaftlichen Gemeinschaft gegenüber. Sie können für ihre eigene Forschung auf den Zugang zu Forschungsdaten Dritter angewiesen sein. Fraglich ist, ob Forschungsdaten unter die **Eigentumsgarantie** fallen (Art. 26 BV). Die Eigentumsgarantie schützt alle vermögenswerten Rechte des Privateigentums, wozu neben den dinglichen Rechten auch die Immaterialgüterrechte gehören.¹¹⁷ Ob auch Daten vom verfassungsrechtlichen Eigentumsbegriff erfasst werden, ist bislang ungeklärt, wird aber eher verneint.¹¹⁸ Betroffen sein kann ferner die **Wirtschaftsfreiheit** (Art. 27 BV) allfälliger Kooperationspartner. Diese schützt die freie privatwirtschaftliche Betätigung, insb. die freie Wahl des Berufes, den freien Zugang zu einer Erwerbstätigkeit und deren freie Ausübung (Art. 27 Abs. 2 BV).¹¹⁹ Im Vordergrund stehen hier die Teilgehalte der freien Ausübung unternehmerischer Tätigkeit und die Vertragsfreiheit. Eine Verpflichtung zur Veröffentlichung von Forschungsdaten nimmt den Kooperationspartnern die Möglichkeit, selbst über die Verwendung der Forschungsdaten zu entscheiden, bspw. durch eine gewinnbringende Lizenzierung oder Veräusserung.

2.2. Einschränkung von Grundrechten

Die Grundrechte gelten nicht absolut, sondern können nach Art. 36 BV eingeschränkt werden. Voraussetzung ist, dass eine gesetzliche Grundlage besteht, die Einschränkung im öffentlichen Interesse liegt

¹¹⁶ MAYA HERTIG, in: Waldmann/Besler/Epiney (Hrsg.), Basler Kommentar, Schweizerische Bundesverfassung (BV), Basel 2015, Art. 20 N 5.

¹¹⁷ BSK BV-VALLENDER/HETTICH, Fn. 116, Art. 26 N 19; GIOVANNI BIAGGINI, in: Biaggini (Hrsg.), BV-Kommentar, Bundesverfassung der Schweizerischen Eidgenossenschaft, Zürich 2017, Art. 26 N 12.

¹¹⁸ THOUVENIN, SJZ 2017, 21 ff., 21; BV Komm.-BIAGGINI, Fn. 117, Art. 26 N 12.

¹¹⁹ BV-Komm., BIAGGINI, Fn. 117, Art. 27 N 4; BSK BV-Uhlmann, Fn. 116, Art. 27 N 4 mit Verweis auf BGE 131 I 333, E. 4 und BGE 137 I 167, E. 3.1.

und verhältnismässig ist (Art. 36 BV). Diese Vorgaben sind bei der konkreten Ausgestaltung einer ORD-Strategie zu berücksichtigen.

Zum einen ist dem Erfordernis einer genügenden **gesetzlichen Grundlage** Rechnung zu tragen, die Verpflichtung zum Zugänglichmachen von Forschungsdaten als ORD sollte idealerweise in einem Gesetz im formellen Sinn verankert sein. Ob eine Verankerung in internen Richtlinien ausreicht, wäre im Einzelfall zu prüfen und hängt auch vom Umfang der Verpflichtung ab. Das **öffentliche Interesse** ist mit dem Interesse der anderen Forschenden und der Allgemeinheit an den Forschungsdaten abzuwägen.

Bei der **Verhältnismässigkeit** sind drei Aspekte zu prüfen: die Eignung, die Erforderlichkeit und die Verhältnismässigkeit im engeren Sinn (Zumutbarkeit). Zum einen müssen in Grundrechte eingreifende Massnahmen geeignet sein, das im öffentlichen Interesse liegende Ziel zu erreichen.¹²⁰ Der Eingriff in ein Grundrecht muss zudem erforderlich sein, darf also nur so weit gehen, wie es zur Erreichung der im öffentlichen Interesse liegenden Ziele erforderlich ist. Zudem müssen die öffentlichen Interessen die entgegenstehenden Grundrechte der Betroffenen überwiegen, es ist also eine Interessenabwägung vorzunehmen. Die Wahrung der Verhältnismässigkeit dürfte bei der Einführung einer ORD-Strategie der entscheidende Punkt sein. Im Hinblick auf die **Eignung** zur Erreichung des öffentlichen Interesses sind Aspekte wie die Zugänglichkeit und die Bedingungen, unter denen Zugang zu den Daten gewährt wird, zu berücksichtigen. Je geringer die Hürden für den Zugang zu den Daten für andere Forschende sind, desto eher wird dem öffentlichen Interesse entsprochen. Bei der **Erforderlichkeit** ist abzuwägen, wie weit die Verpflichtung gehen muss, um das mit der Regelung verfolgte öffentliche Interesse zu erreichen; es ist jeweils die mildeste Massnahme zu wählen. Dies bedeutet, dass die Grundrechte der betroffenen Forschenden und Kooperationspartner so weit wie möglich zu wahren sind; dazu gehören neben der Forschungsfreiheit auch die Eigentumsgarantie und die Wirtschaftsfreiheit, die durch eine Regelung betroffen sind, welche die freie Verfügbarkeit über allenfalls an Forschungsdaten bestehende Immaterialgüterrechte und den Schutz von Forschungsdaten als Geschäftsgeheimnisse einschränken.¹²¹ Diese Punkte dürften auch bei der Beurteilung der Verhältnismässigkeit im engeren Sinn von Bedeutung sein.

¹²⁰ BV-Komm., BIAGGINI, Fn. 117, Art. 5 N 21 mit Verweis auf BGE 136 I 29, E. 4.2; BSK BV-EPINEY, Fn. 116, Art. 5 N 70.

¹²¹ Siehe dazu vorne, B.1.5.

3. Lizenzverträge

3.1. Gegenstand

Mit einem **Lizenzvertrag** ermächtigt der Lizenzgeber die Lizenznehmerin, ein Immaterialgut im vereinbarten Umfang zu nutzen.¹²² Ein Entgelt (Lizenzgebühr oder Royalty) gehört nicht zum objektiv wesentlichen Vertragsinhalt, wird aber regelmässig vereinbart.¹²³ Mit einem Lizenzvertrag kann die **Nutzung aller Arten von immateriellen Gütern** erlaubt werden.

Ein echter Lizenzvertrag liegt vor, wenn das immaterielle Gut, dessen Nutzung lizenziert wird, durch ein Immaterialgüterrecht (bspw. ein Patent oder ein Urheberrecht) geschützt ist. Mit einem unechten Lizenzvertrag wird die Nutzung eines nicht (oder nicht mehr) durch ein Immaterialgüterrecht geschützten immateriellen Gutes geregelt,¹²⁴ insb. die Nutzung von Know-how. Dazu gehören namentlich die Informationen, die als Fabrikations- und Geschäftsgeheimnisse durch Art. 6 UWG und Art. 162 StGB gegen die unbefugte Nutzung durch Dritte geschützt sind. Wird neben der Nutzung von absolut-rechtlich geschützten Immaterialgütern auch die Nutzung von (ergänzendem) Know-how erlaubt, liegt ein gemischter Lizenzvertrag vor.¹²⁵ **Lizenzverträge über Daten** sind in der Regel als **unechte Lizenzverträge** zu qualifizieren; repräsentieren die Daten urheberrechtlich geschützte Werke oder Leistungen, liegt ein gemischter Lizenzvertrag vor.

3.2. Form

Der Abschluss eines Vertrags ist nur an eine Form gebunden, wenn dies gesetzlich vorgesehen oder von den Parteien vereinbart wurde (Art. 11 Abs. 1 und Art. 16 Abs. 1 OR). Da es sich beim Lizenzvertrag um einen gesetzlich nicht geregelten Vertrag handelt (sog. Innominatkontrakt), sieht das Gesetz auch **keine Formvorschriften** vor. Haben die Parteien nichts anderes vereinbart, kann ein Lizenzvertrag also auch in rein elektronischer Form, mündlich oder durch konkludentes Verhalten abgeschlossen werden.¹²⁶

¹²² Reto HILTY, Lizenzvertragsrecht, Bern 2002, 5 ff.; BSK OR I-AMSTUTZ/MORIN, Fn. 106, Einl. vor OR 184 ff. N 238; ROLAND VON BÜREN, in: David/von Büren (Hrsg.), Schweizerisches Immaterialgüter- und Wettbewerbsrecht (SIWR), I/1, Grundlagen, Basel 2002, 295.

¹²³ BSK OR I-AMSTUTZ/MORIN, Fn. 106, Einl. vor OR 184 ff. N 238; EUGEN MARBACH/PATRIK DUCREY/GREGOR WILD, Immaterialgüter- und Wettbewerbsrecht, Bern 2017, Rn. 925; MAGDA STREULI-YOUSSEF, in: Streuli-Youssef (Hrsg.), Schweizerisches Immaterialgüter- und Wettbewerbsrecht (SWIT), V/1, Basel 2020, 22.

¹²⁴ ROBERT M. STUTZ/STEPHAN BEUTLER/MARC HOTTINGER, in: Stutz/Bleuler/Hottinger (Hrsg.), Stämpflis Handkommentar, Designgesetz (DesG), Bern 2022, Art. 15 N 12; CLAIRE HUGUENIN, Obligationenrecht, Allgemeiner und Besonderer Teil, Zürich 2019, Rn. 3792; HILTY, Fn. 122, 15.

¹²⁵ ROLAND FISCHER/LARA DORIGO, in: Weinmann/Münch/Herrn (Hrsg.), Schweizer IP-Handbuch, Intellectual Property – Konzepte, Checklisten und Musterdokumente für die Praxis, Basel 2021, § 17 Rz. 0.8.

¹²⁶ HILTY, Fn. 122, 275; VON BÜREN, Fn. 122, 332; SHK DesG-STUTZ/BEUTLER/HOTTINGER, Fn. 124, Art. 15 N 21.

3.3. Inhalt

Das Vertragsrecht beruht auf dem Grundsatz der Vertragsfreiheit. Diese umfasst die Freiheit der inhaltlichen Ausgestaltung von Verträgen, sog. **Inhaltsfreiheit**.¹²⁷ Im Rahmen der allgemeinen Grenzen der Vertragsfreiheit (insb. Art. 19/20 OR und Art. 27 ZGB)¹²⁸ können die Parteien **Lizenzverträge frei ausgestalten**. Das gilt auch für ORD. Die Institutionen des ETH-Bereichs können damit die Bedingungen der Lizenzverträge, unter denen Forschungsdaten als ORD zugänglich gemacht werden, frei gestalten.

Namentlich ist es möglich, die Lizenz unentgeltlich (sog. Gratis- oder Freilizenz) oder nur gegen Bezahlung einer **Lizenzgebühr** zu erteilen. Auch die Ausgestaltung der Lizenzgebühr steht den Parteien frei. In der Praxis finden sich zahlreiche Varianten zur Bestimmung und Berechnung von Lizenzgebühren, so etwa: einmalige Lizenzgebühren, Meilenstein-Pauschalzahlungen bei Erreichen gewisser Ziele, periodische Gebühren, umsatz- oder gewinnabhängige Gebühren sowie Stücklizenzen.¹²⁹ Häufig verbinden die Parteien eine beim Vertragsabschluss zu zahlende Pauschale (sog. *downpayment*) mit einer periodisch (z.B. jährlich oder quartalsweise) zu leistenden, umsatzabhängigen Lizenzgebühr.¹³⁰

Auch der Umfang der mit der Lizenz eingeräumten **Nutzungsrechte** kann von den Parteien frei bestimmt werden. Namentlich kann die Nutzung zeitlich (bspw. nur für ein Jahr) oder örtlich (bspw. nur in einem bestimmten Land) oder auf die Nutzung zu bestimmten Zwecken (bspw. nur für rein wissenschaftliche Zwecke unter Ausschluss einer kommerziellen Nutzung) eingeschränkt werden.

Zudem kann (und sollte) geregelt werden, ob die Lizenznehmerin berechtigt ist, Dritten eine **Unterlizenz** zu erteilen, die diese zur Nutzung des immateriellen Gutes berechtigt. Die Unterlizenz kann dabei keine weitergehenden (aber weniger weit gehende) Befugnisse umfassen als die Hauptlizenz. Da umstritten ist, ob die Lizenznehmerin zur Erteilung einer Unterlizenz berechtigt ist, wenn der Lizenzvertrag dazu keine Regelung enthält,¹³¹ sollte die Frage auch (und gerade) dann ausdrücklich geregelt werden, wenn die Lizenznehmerin nicht zur Erteilung einer Unterlizenz berechtigt sein soll.

¹²⁷ BSK OR I-MEISE/HUGUENIN, Fn. 111, Art. 19/20 N 5 f. mit Verweis auf BGE 115 II 237, E. 4.d; PETER GAUCH/WALTER R. SCHLUEP/JÖRG SCHMID/SUSAN EMMENEGGER, Schweizerisches Obligationenrecht Allgemeiner Teil, Zürich 2020, Rz 626.

¹²⁸ Siehe dazu vorne, C.4.

¹²⁹ Zu den verschiedenen Varianten: FISCHER/DORIGO, Fn. 125, § 17 Rz. 6.1; VON BÜREN, Fn. 122, 347 ff.; HILTY, Fn. 122, 486.

¹³⁰ Eingehend zum sog. «downpayment» FISCHER/DORIGO, Fn. 125, § 17 Rz. 6.3 f.

¹³¹ HILTY, Fn. 122, 758 ff.; VON BÜREN, Fn. 122, S. 314 ff.; SHK DesG-STUTZ/BEUTLER/HOTTINGER, Fn. 124, Art. 15 N 15.

4. Kartellrechtliche Aspekte

Bei der Umsetzung von ORD müssen gewisse kartellrechtliche Vorgaben beachtet werden. Das Kartellgesetz findet Anwendungen auf Unternehmen des privaten und des öffentlichen Rechts, die sich am Wettbewerb beteiligen. Nicht dem Kartellgesetz unterstehen grundsätzlich Privatpersonen.¹³² Auf Forschende, welche ihre Daten öffentlich machen, kommt das Kartellrecht deshalb nicht zur Anwendung. Die Betreiber von ORD-Plattformen dürften dagegen dem Kartellrecht unterstehen.

Je nach Zugangsbedingungen können aus Sicht der Betreiber von ORD-Plattformen Probleme auftreten, wenn ein Betreiber als relativ marktmächtiges oder marktbeherrschendes Unternehmen qualifiziert würde. Ein Unternehmen gilt nach Art. 4 Abs. 2 KG als **marktbeherrschend**, wenn es auf einem Markt in der Lage ist, sich in wesentlichem Umfang unabhängig zu verhalten. Ein wesentlicher Faktor zur Beurteilung, ob eine Marktbeherrschung vorliegt, ist der Marktanteil; dieser müsste – besondere Umstände¹³³ vorbehalten – über 50% liegen, damit von einer Marktbeherrschung ausgegangen werden kann.¹³⁴ Da Forschungsdaten überall auf der Welt erhoben und bearbeitet werden, ist kaum davon auszugehen, dass eine ORD-Plattform als marktbeherrschend qualifiziert wird. Naheliegender ist das Vorliegen von relativer Marktmacht. Ein Unternehmen gilt nach Art. 4 Abs. 2^{bis} KG als **relativ marktmächtig**, wenn andere Unternehmen von diesem in einer Weise abhängig sind, dass keine ausreichenden und zumutbaren Ausweichmöglichkeiten bestehen. Auch in dieser Hinsicht ist zu untersuchen, ob die in Frage stehenden Forschungsdaten als substituierbar angesehen werden können. Forschungsdaten, die bspw. zum Stand der Technik bzw. Forschung gehören und sich deshalb auch in anderen Quellen finden, sind substituierbar. Bei nicht substituierbaren Forschungsdaten bestehen für andere Forschende keine Ausweichmöglichkeiten, weshalb eine relative Marktmacht vorliegen dürfte, wenn diese Forschungsdaten durch eine Forschungsinstitution als ORD angeboten werden.

Das Innehaben einer relativ marktmächtigen oder marktbeherrschenden Stellung ist für sich nicht unzulässig, unzulässig sind nur gewisse **missbräuchliche Verhaltensweisen** (Art. 7 Abs. 1 f. KG). Einschlägig sein kann Art. 7 Abs. 2 lit. a KG. **Verweigert** die Inhaberin einer wesentlichen Einrichtung oder von Informationen (*Essential Facilities*) **Dritten den Zugang**, ohne dass dafür sachliche Gründe (*Legitimate Business Reasons*) vorliegen, kann eine unzulässige Geschäftsverweigerung vorliegen. Eine

¹³² BERNHARD RUBIN/MATTHIAS COURVOISIER, in: Baker & McKenzie (Hrsg.), Stämpfli Handkommentar, Kartellgesetz (KG), Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen, Bern 2007, Art. 2 N 9; RETO HEIZMANN/MICHAEL MAYER, in: Zäch et al. (Hrsg.), KG-Kommentar, Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen, Zürich 2018, Art. 2 N 25.

¹³³ Solche besonderen Umstände könnten bspw. vorliegen, wenn gewisse Daten nur bei einer Forschungsinstitution exklusiv erhoben werden können und diese eine Verpflichtung vorsieht, die Daten exklusiv auf ihrer Plattform bereitzustellen.

¹³⁴ JÜRGEN BORER, in: Orell Füssli Kommentar, Wettbewerbsrecht I, Schweizerisches Kartellgesetz (KG) mit den Ausführungserlassen sowie einschlägigen Bekanntmachungen und Meldeformularen der WEKO, Zürich 2011, Art. 4 N 19; SHK KG-ROLAND KÖCHLI/PHILIPPE M. REICH, Fn. 132, Art. 4 N 38.

wesentliche Einrichtung liegt immer dann vor, wenn der Zugang dazu objektiv notwendig ist, um auf einem nachgelagerten Markt tätig zu werden.¹³⁵ Ob eine ORD-Plattform als wesentliche Einrichtung gilt, ist im Einzelfall zu prüfen. Ein Verstoss gegen Art. 7 Abs. 2 lit. a KG würde nur vorliegen, wenn der Zugang zu bestimmten Forschungsdaten für bestimmte Personengruppen eingeschränkt wird, ohne dass dafür sachliche Gründe vorgebracht werden können.

Ein missbräuchliches Verhalten könnte auch in der **Festlegung unangemessener Preise oder unangemessener Geschäftsbedingungen** bestehen (Art. 7 Abs. 2 lit. c KG) bspw., wenn für den Zugang zu den Daten ein (hoher) Preis verlangt wird oder wenn der Zugang zur ORD-Plattform an besonders strenge Bedingungen geknüpft ist, die sich von den Bedingungen anderer ORD-Plattformen wesentlich unterscheiden. Ob dieser Tatbestand erfüllt ist, wäre im Einzelfall zu klären. Zur Höhe des Nutzungsentgelts sei dennoch gesagt, dass eine Beschränkung des Zugangs aus wirtschaftlichen Gründen durch die Erhebung eines Nutzungsentgelts aus kartellrechtlicher Sicht zulässig ist, sofern es dabei um den Ausgleich eines finanziellen Aufwands im Zusammenhang mit der Bereitstellung der Daten geht. Darunter können namentlich Kosten aus der Zusammenführung von Datensätzen, der Anonymisierung oder der Herstellung von Interoperabilität erfasst werden.¹³⁶

5. Lizenzen für ORD

5.1. Abschluss

Die Vertragsfreiheit umfasst auch die Freiheit, einen Vertrag mit einer Partei abzuschliessen oder nicht abzuschliessen, sog. **Abschlussfreiheit**.¹³⁷

Aus rechtlicher Sicht sind die Anbieter von ORD nicht verpflichtet, mit Dritten einen Lizenzvertrag über die Nutzung von Forschungsdaten abzuschliessen und sie sind grundsätzlich frei, bei Anfrage eines Dritten das **Erteilen einer Lizenz zu verweigern**. Sie können namentlich vorsehen, dass bestimmten Dritten keine Lizenzen erteilt werden, bspw. Unternehmen, die kommerzielle Forschung betreiben, oder Hochschulen aus bestimmten Ländern. Gewisse Einschränkungen der Abschlussfreiheit können sich zwar aus dem Kartellrecht ergeben, die Voraussetzungen für einen Kontrahierungszwang sind aber hoch und werden nur in seltenen Fällen erfüllt sein.¹³⁸

¹³⁵ MARC AMSTUTZ/BLAISE CARRON, in: Amstutz/Reinert (Hrsg.), Basler Kommentar, Kartellgesetz (KG), Basel 2021, Art. 7 N 181 und 248; RAMIN SILVAN GOHARI, Die Essential Facilities-Doktrin, sic! 2019, 533 ff., 535, 539, je m.w.H.

¹³⁶ ALFRED FRÜH, Datenzugangsrechte, sic! 2018 521 ff., 528 ff.

¹³⁷ BSK OR I-MEISE/HUGUENIN, Fn. 106, Art. 19/20 N 8 mit Verweis auf BGE 129 III 35, E. 6.1; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, Fn. 127, Rz 721 ff., 1102 ff.

¹³⁸ Siehe dazu vorne, D.4.

5.2. Ausgestaltung

Bei der Ausgestaltung der Lizenzverträge sind die Anbieter von ORD grundsätzlich frei.¹³⁹ Die nahezu uneingeschränkte inhaltliche Freiheit ermöglicht es, Lizenzverträge über ORD so auszugestalten, dass sie mit dem Konzept von ORD und mit den FAIR-Prinzipien übereinstimmen.

Aus rechtlicher Sicht ist es ohne weiteres möglich, die Erteilung einer Lizenz für ORD vom Bezahlen einer **Lizenzgebühr** abhängig zu machen. Im Vordergrund steht dabei wohl eine einmalige Gebühr, die beim Erteilen der Lizenz und beim Gewähren des Zugangs zu den Daten zu zahlen ist. Denkbar ist auch, von Unternehmen die Zahlung einer Lizenzgebühr zu verlangen und Hochschulen sowie anderen Forschungsinstitutionen Gratislizenzen zu erteilen.

Die Anbieter von ORD können den **Umfang** der mit einer Lizenz eingeräumten **Nutzungsrechte** frei festlegen. Denkbar ist namentlich eine Einschränkung auf nicht-kommerzielle Nutzungen. Möglich ist auch, den Lizenznehmerinnen weitere Verpflichtungen aufzuerlegen, bspw. die Verpflichtung, die aus den Daten gewonnenen Erkenntnisse oder die bei der Nutzung von ORD generierten Daten ebenfalls frei zugänglich zu machen.

Die Anbieter von ORD sollten regeln, ob die Lizenznehmerinnen zur Erteilung von **Unterlizenzen** berechtigt sind. Das Einräumen einer solchen Befugnis ist zwar möglich, scheint aber wenig sinnvoll, wenn der Anbieter von ORD eine gewisse Kontrolle über die Nutzung der Forschungsdaten erhalten will. Wer an der Nutzung der Daten interessiert ist, kann jederzeit vom Anbieter von ORD direkt eine Lizenz erhalten. Mit diesem Ansatz hat der Anbieter von ORD Kenntnis, wer zur Nutzung der Forschungsdaten berechtigt ist.

5.3. Standardlizenzen

Lizenzverträge können zwischen den Parteien frei ausgehandelt und ausgestaltet werden. Nutzen sie diese Freiheit und schliessen sie einen Vertrag, der spezifische Regeln für den konkreten Fall enthält, liegt eine **Individualvereinbarung** vor. In vielen Konstellationen werden allerdings Standardlizenzverträge verwendet, die von einer Partei vollständig vorformuliert und von der anderen Partei «as is» akzeptiert werden. Solche Standardlizenzverträge sind bspw. die Creative Commons-Lizenzen¹⁴⁰ oder die von der Open Knowledge Foundation entwickelten Lizenzen.¹⁴¹

¹³⁹ Siehe dazu gerade vorstehend, D.5.2.

¹⁴⁰ Siehe dazu <<https://www.creativecommons.ch>> (zuletzt besucht am 28. Juni 2024).

¹⁴¹ Siehe dazu <<https://opendatacommons.org/licenses/>> (zuletzt besucht am 28. Juni 2024).

5.3.1. Open Database License

Die Open Knowledge Foundation hat **drei Standardlizenzen für Datenbanken** geschaffen: die Open Database License (ODbL), die Open Data Commons Attribution License (ODC-By) und die Open Data Commons Public Domain Dedication and License (PDDL).¹⁴² Diese Lizenzen erfassen allerdings nur die Urheberrechte und die *sui generis*-Rechte an Datenbanken.¹⁴³ Andere Rechte, insb. allfällige Rechtsansprüche, die sich aus dem Datenschutzrecht oder aus einem Verstoss gegen die Pflicht zur Geheimhaltung der Daten ergeben,¹⁴⁴ werden nicht erfasst. In vielen Fällen sind diese Lizenzen deshalb für ORD nicht geeignet.

Die **Open Data Commons Public Domain Dedication and License (PDDL)** erlaubt die **Nutzung von Datenbanken und ihren Inhalten** umfassend. Rechtlich handelt es sich um eine Kombination aus Verzichtserklärung und Lizenz. Die PDDL erfasst sowohl die Urheberrechte und das *sui-generis*-Recht an der Datenbank als auch die Rechte am Inhalt der Datenbank (Art. 2.2 PDDL). Mit der PDDL stellt der Rechteinhaber die Datenbank und ihre Inhalte ins **Gemeingut** («*public domain*») (Art. 3.1 PDDL). Soweit dies nicht möglich ist, weil gewisse Länder eine Widmung zum Gemeingut nicht zulassen, verzichtet der Rechteinhaber auf seine Urheberrechte und das *sui-generis* Recht (Art. 3.2 PDDL). Soweit auch dies nicht möglich ist, weil gewisse Länder einen Verzicht auf Urheberrechte nicht zulassen, erteilt der Rechteinhaber an der Datenbank und ihren Inhalten eine umfassende Lizenz (Art. 3.3 PDDL). Die PDDL unterwirft die Lizenznehmerinnen keinerlei Restriktionen bei der Nutzung der Datenbank.

Die **Open Data Commons Attribution License (ODC-By)** erlaubt die **Nutzung von Datenbanken**, die durch das Urheberrecht oder durch das *sui-generis*-Recht für Datenbanken geschützt sind (Art. 2.1 f. ODC-By). Sie bezieht sich aber nur auf die Rechte an den Datenbanken, **nicht** auf allfällige Rechte an den **Inhalten von Datenbanken**, insb. auf allfällige Urheber- oder Leistungsschutzrechte an in der Datenbank enthaltenen Werken oder Leistungen; auch Ansprüche aus dem Datenschutz- oder Persönlichkeitsrecht werden nicht von der Lizenz erfasst (Art. 2.4 ODC-By). Die ODC-By enthält nur eine Pflicht zur **«attribution»** (Art. 4.3 ODC-By). Die Erteilung von **Unterlizenzen** ist ausgeschlossen (Art. 4.4 Satz 1 ODC-By). Stattdessen bietet der Lizenzgeber Dritten, welche die unter der Lizenz verbreitete Datenbank (oder Teile davon) in veränderter oder unveränderter Form von der Lizenznehmerin erhalten haben, die Erteilung einer ODbL an (Art. 4.4 Satz 2 ODC-By).

Die **Open Database License (ODbL)** enthält teilweise dieselben Vorgaben wie die ODC-By, sieht aber weitergehende Restriktionen vor. Wie die ODC-By erlaubt die ODbL die **Nutzung von Datenbanken**,

¹⁴² Siehe dazu <<https://opendatacommons.org/licenses/>> (zuletzt besucht am 28. Juni 2024).

¹⁴³ Siehe dazu vorne, B.1.2. und B.1.3.

¹⁴⁴ Siehe dazu vorne, B.3 und B.1.5.

(Art. 2.1 f. ODbL). Wie die ODC-By bezieht sie sich aber nur auf die Rechte an den Datenbanken, nicht auf die allfälligen Rechte an den Inhalten von Datenbanken (Art. 2.4 ODbL). Die ODbL enthält neben der Pflicht zur **«attribution»** (Art. 4.3 ODbL) auch eine Pflicht zum **«share alike»** (Art. 4.4 ODbL). Zudem sieht die ODbL vor, dass Datenbanken offengehalten (**«keep open»**) werden müssen (Art. 4.7.a ODbL). Dritte dürfen eine Datenbank, die sie nach Massgabe der ODbL nutzen dürfen, zwar durch Nutzungsbedingungen oder technische Massnahmen gegen Zugriffe und Nutzungen durch Dritte schützen, aber nur, wenn sie dem Empfänger der mit solchen Restriktionen verbundenen Datenbank zugleich eine restriktionsfreie Kopie der Datenbank zugänglich machen, sog **«parallel distribution»** (Art. 4.7.b ODbL). Wie bei der ODC-By ist die Erteilung von **Unterlizenzen** auch bei der ODbL ausgeschlossen (Art. 4.8 ODbL).

5.3.2. Creative Commons-Lizenzen

Creative Commons-Lizenzen sind ein wirksames Instrument, um auf einfache Weise den Umfang der Rechte festzulegen, die den Nutzern in Bezug auf ein urheberrechtlich geschütztes Werk eingeräumt werden. Creative Commons-Lizenzen haben eine hohe Akzeptanz erlangt und ihre Verwendung wird von vielen öffentlichen Einrichtungen empfohlen.¹⁴⁵ Die Rechteinhaber können festlegen, wie ihre Inhalte verwertet werden, indem sie aus sechs Creative Commons-Lizenzkategorien wählen.

Die freizügigste Lizenz ist die sog. **Attribution License (CC BY)**. Sie bietet jedem Nutzer die Freiheit, die Daten weiterzuverwenden, sofern er die ursprünglichen Inhaber nennt und angibt, ob Änderungen am ursprünglichen Inhalt vorgenommen wurden. Die sog. **«Share Alike» License (CC BY-SA)** erfordert die Angabe der Quelle und die Nutzung eines neu erstellten auf der Grundlage eines bereits existierenden Werks unter derselben Lizenz. Die sog. **«Non Commercial» License (CC BY-NC)** sieht dieselben Rechte vor wie die Attribution License (CC-BY), schliesst aber jegliche Nutzung für kommerzielle Zwecke aus. Die sog. **«No Derivatives» License (CC BY-ND)** erlaubt die kommerzielle Nutzung, verbietet aber jegliche Änderung von abgeleiteten Werken.

Die **Creative Commons Zero License (CC0)** ist eine Kombination aus Verzichtserklärung und Lizenz. Mit der CC0 erklärt der «Affirmer» einen **umfassenden Verzicht** auf seine Urheberrechte und ähnlichen Rechte (Art. 2 CC0). Diese Rechte werden in der CC0 umfassend definiert; dazu gehören namentlich (aber nicht nur): urheberrechtliche Nutzungsrechte, Urheberpersönlichkeitsrechte, Persönlichkeitsrechte, Ansprüche aus UWG, *sui-generis*-Datenbankrechte und ähnliche Rechte (Art. 1 CC0).

¹⁴⁵ Siehe z.B. die Empfehlungen der Open-Access-Infrastruktur für die Forschung in Europa (OpenAIRE), abrufbar unter <https://zenodo.org/record/2574619> (zuletzt besucht am 27. Mai 2024), welche die Verwendung von Creative Commons CC BY 4.0-Lizenzen empfiehlt, wenn das Material ein Werk im Sinn des URG darstellt, und die Verwendung der CC0-Lizenz für Daten und Datensätze die nicht als Datenbanken strukturiert sind.

Soweit dieser Verzicht nicht gültig sein sollte, erteilt der «Affirmer» eine umfassende, unentgeltliche und unwiderrufliche Lizenz zur Nutzung aller Rechte (Art. 3 CC0). Daten, die unter einer CC0-Lizenz veröffentlicht werden, können damit frei und ohne Einschränkungen genutzt, verändert und weiterverwendet werden. Die CC0 ist ein wirksames Instrument für das Schaffen von Rechtssicherheit, weil sie klarstellt, dass damit gekennzeichnete **Inhalte frei verwendet werden dürfen**. Sie hat zudem den Vorteil, dass sie das Problem des «Attribution Stacking» löst, d.h. die Notwendigkeit, eine grosse Anzahl von wiederverwendeten Datensätzen zu nennen. Die Anwendung einer CC0-Lizenz gibt den Nutzern damit die Möglichkeit, mehrere Datensätze zusammenzufassen, ohne sich um die Nennung der einzelnen Rechteinhaber kümmern zu müssen.

5.3.3. Durchsetzung

Lizenzverträge werden immer zwischen einem (oder mehreren) Lizenzgebern und einer (oder mehreren) Lizenznehmerin(nen) abgeschlossen. Der Lizenzgeber ist Inhaber der Rechte, die von der Lizenznehmerin im Rahmen und auf der Grundlage des Lizenzvertrags genutzt werden dürfen. Hält sich die Lizenznehmerin nicht an die Vorgaben des Lizenzvertrags, kann der Lizenzgeber seine vertraglichen Rechte gegenüber der Lizenznehmerin durchsetzen. Lizenzverträge enthalten bisweilen Regelungen zur Rechtsdurchsetzung, bspw. zur Aufhebung oder Kündigung bei Vertragsverletzung; werden diese Fragen von den Parteien nicht geregelt, kommen die allgemeinen Vorschriften über die Vertragsverletzung (Art. 97 ff. OR und Art. 192 ff. sowie Art. 367 ff. OR analog) zur Anwendung. Das gilt für Individual- ebenso wie für Standardlizenzverträge. Da für das Zugänglichmachen von Forschungsdaten als ORD die Verwendung der **Creative Commons Lizenzen CC-BY und CC0** vorgeschlagen wird, wird hier nur die Durchsetzung dieser beiden Lizenzen kurz skizziert.

Die **CC-BY-Lizenz** sieht eine Reihe von vertraglichen Verpflichtungen der Lizenznehmerin vor, etwa die Pflicht, den oder die Urheber zu nennen oder die Pflicht, einen Hinweis auf den urheberrechtlichen Schutz («copyright notice»), auf die Lizenz und auf den Haftungsausschluss («disclaimer of warranties») anzubringen (Sec. 3.a.1.A CC-BY). Zudem darf die Lizenznehmerin den Lizenzgegenstand nicht unter anderen oder zusätzlichen Bedingungen anbieten (Sec. 2.5.B CC-BY). Wird eine vertragliche Verpflichtung verletzt, bspw. weil die Urheberin nicht genannt wird, endet die Lizenz automatisch (Sec. 6.a CC-BY). Eine Klage auf **Erfüllung der vertraglichen Verpflichtungen** ist damit ausgeschlossen, weil der Lizenzvertrag mit der Verletzung endet und die ehemalige Lizenznehmerin mit dem Dahinfallen des Vertrags nicht mehr auf dessen Erfüllung in Anspruch genommen werden kann. Eine Klage auf **Schadenersatz** ist zwar möglich (Sec. 6.b CC-BY), in der Regel wird es aber an einem Schaden fehlen.

Anders als die CC-BY-Lizenz sieht die **CC0-Lizenz** keine vertraglichen Verpflichtungen der Lizenznehmerin vor. Diese kann die CC0-Lizenz damit nicht verletzen und die Frage der Durchsetzung vertraglicher Ansprüche stellt sich nicht.



Zur **Durchsetzung** der Standardlizenzen CC-BY und CC0 ist der **Rechteinhaber und Lizenzgeber berechtigt**. Rechteinhaber an ORD ist gemäss Art. 36 ETH-Gesetz die Institution des ETH-Bereichs; anderes gilt nur für Urheberrechte.¹⁴⁶ Zur Durchsetzung der Standardlizenzen ist damit die jeweilige Institution des ETH-Bereichs befugt. Enthalten die ORD auch urheberrechtlich geschützte Werke, kann eine Standardlizenz für die Gesamtheit der Daten nur von der Institution und den Inhabern der Urheberrechte gemeinsam erteilt werden. Die beiden (oder mehreren) Lizenzgeber können aber selbständig gegen eine Vertragsverletzung vorgehen und ihren Anteil an einem allfälligen Schaden geltend machen.

¹⁴⁶ Siehe dazu vorne, B.2.



Open Research Data

Legal restrictions and options for safeguarding legal rights

Prof Dr Florent Thouvenin

Dr Stephanie Volz

with the collaboration of:
MLaw Deborah De Col, RA and
MLaw Samuel Mätzler, RA

Zurich, 24 March 2025

The original version is in German. Translated by Architext Zürich.



TABLE OF CONTENTS

A.	Introduction	5
1.	Mandate	5
2.	Definitions	5
B.	Basics	6
1.	Rights to data.....	6
1.1.	No ownership rights	6
1.2.	Copyright	7
1.3.	Sui generis rights to databases in the EU.....	10
1.4.	Direct taking over of work products (Art. 5 (c) UCA)	12
1.5.	Protection of manufacturing and trade secrecy (know-how / proprietary information) 13	
2.	Rightholder status	16
3.	Data protection law	18
C.	Restrictions on ORD.....	20
1.	Question presented and approach taken	20
2.	Legal restrictions.....	21
2.1.	Export control	21
2.2.	Information security law	22
2.3.	Health law	24
2.3.1.	General remarks	24
2.3.2.	The area of human research	24
2.3.3.	Non-human research area	27
2.3.4.	Further legislation	27
2.4.	Genetic technology	28
2.5.	Environmental law	29
2.6.	Chemicals law	30
2.7.	Food law	31
2.8.	Energy and nuclear energy law.....	31
2.9.	Animal welfare law.....	33
2.10.	Financial markets law.....	33
3.	Third party rights.....	34
3.1.	Copyright.....	34
3.2.	Patents	35
3.3.	Claims arising from the protection of secrets under criminal law	36
3.4.	Claims arising from UCA	36
3.5.	Data protection claims	37
4.	Contractual restrictions	38



5. Liability	39
D. Legal implementation of ORD	40
1. Preliminary remarks	40
2. Constitutional framework	41
2.1. Fundamental rights relevant to ORD	41
2.2. Restriction on fundamental rights	41
3. Licence agreements	42
3.1. Subject matter	42
3.2. Formal requirements	43
3.3. Content	43
4. Competition law aspects	44
5. Licences for ORD	46
5.1. Conclusion of a contract.....	46
5.2. Drafting/structuring the agreement	46
5.3. Standard licences	47
5.3.1. Open Database Licence	47
5.3.2. Creative Commons licences	48
5.3.3. Enforcement	49



EXECUTIVE SUMMARY

Where employees of one of the institutions from the ETH Domain generate data in the course of their employment, the institution in question is entitled to assert rights in that data. A different rule will apply only in the case of copyright to literary and artistic works which are represented in data. This means that the institutions can generally determine how and in what form data are to be made accessible as ORD. However, ORD are subject to certain restrictions. These may arise from applicable law, third-party rights or contract.

Although we make no claim to comprehensiveness, our analysis of possible legal restrictions has shown that there are provisions in export control law, information security law, health law, genetic engineering law, environmental law, chemicals law, food law, energy and nuclear energy law, and financial market law that may prevent research data from being made accessible as ORD. In addition to legal restrictions, account must also be taken of possible third-party rights. Of particular relevance here are copyright claims, e.g. for copyright-protected elements of a data record or for certain databases, as well as claims arising from the protection of manufacturing and trade secrets (Art. 162 Criminal Code [SCC] and Art. 6 Unfair Competition Act [UCA]), from the Unfair Competition Act generally (Art. 5 (c) UCA) and from provisions of data protection law.

In addition, contracts with other universities or companies may contain provisions on the handling of data, in particular confidentiality obligations, which must be complied with in connection with ORD.

Implementation of an ORD strategy must be undertaken within the framework of Swiss constitutional law. A legal obligation to make data publicly accessible can affect and possibly violate academic freedom, freedom of property and freedom to engage in commerce. In addition, competition law rules may be relevant, in particular with regard to the duty to make data available and with regard to possible pricing.

ORD providers are generally legally free to draft licence agreements that allow third parties to use the data. In individual agreements, they can impose obligations on licensees, e.g. to pay a royalty. However, it will generally make sense to use standard licences, in particular the Creative Commons Zero License (CC0) or the Creative Commons Attribution License (CC-BY).



A. INTRODUCTION

1. Mandate

The ETH Domain comprises six independent institutions: the Swiss Federal Institute of Technology Zurich (ETH Zurich), the École polytechnique fédérale Lausanne (EPFL), the Paul Scherrer Institute (PSI), the Swiss Federal Laboratories for Materials Science and Technology (Empa), the Swiss Federal Institute for Forest, Snow and Landscape Research (WSL) and the Swiss Federal Institute of Aquatic Science and Technology (Eawag). The two academic institutions (ETH and EPFL) and the four research institutes (PSI, Empa, WSL and EAWAG) within the ETH Domain are independent institutions with their own legal personality. Their activities are governed by federal law.

In May 2020, the ETH Board adopted an *Open Research Data Position within the ETH Domain* and established an *Open Research Data Program*. That program comprises five measures. Measure four deals with the legal basis for Open Research Data (ORD). Three objectives are pursued as part of this measure:

- Identification of the legal obstacles (at the federal level) confronting researchers or institutions within the ETH Domain making research data accessible as ORD;
- Delineation of the scope of responsibilities of researchers and institutions within the ETH Domain;
- Development of ORD guidelines that can be used as a common reference within the ETH Domain.

At the end of 2023, the Center for Information Technology, Society, and Law (ITSLS) at the University of Zurich was given a mandate by WSL to work on the implementation of measure four. This report, which analyses the issues arising from the first two objectives of measure four, is limited to Swiss federal law; the only exception is the so-called *sui generis* law of EU databases. The focus of our analysis is on factual data. However, as it is often not possible to clearly separate personal and factual data, the analysis also takes account of issues under data protection law. Our comments on data protection law are limited to the Swiss Data Protection Act (DPA); the analysis does not cover the provisions of the EU General Data Protection Regulation (GDPR).

2. Definitions

This report is based on the following definitions:

- **Research data** are all data the relevant scientific community considers necessary to validate research results. Such data may be (and are intended to be) used on other research projects.

The definition encompasses raw data, processed data and metadata. The legal system as a whole does not generally distinguish between these types of data; such distinctions are only made in the context of a few enactments. Thus, only the broader definition of research data is used in this report.

- **FAIR principles** are internationally recognised guidelines for improving the findability, accessibility, interoperability and reusability of digital content.
- **Open Research Data (ORD)** are research data that complies with the FAIR principles and are publicly available, accessible and reusable for at least 10 years. Source code is generally not covered by this definition. A different rule applies only if research data without (specific) source code cannot be used for validation of research results or for further use in other research projects. It should also be noted that research data and source code cannot always be clearly separated; for example, the "weights" in trained deep neural networks can be seen as code or as data.

B. BASICS

1. Rights to data

1.1. No ownership rights

The question of whether and under what conditions research data can be made freely accessible depends fundamentally on the question of whether the data "belong to someone", i.e. whether ownership rights to data exist. This question, when posed in this way, can be answered clearly: Swiss law **does not recognise ownership rights to data**, irrespective of whether the data are factual or personal.¹ Ownership rights within the meaning of property law only exists with respect to an item of property. An item of property is a physical, delimited object that is accessible to human control.² Data lacks physicality because they are not tangible. An item of property is, for example, a data carrier, but not the data stored on this carrier.

¹ ROLF H. WEBER/FLORENT THOUVENIN, Dateneigentum und Datenzugangsrechte - Bausteine der Informationsgesellschaft?, ZSR 2018, 43 et seq., 49; ALAIN SCHMID/KIRSTEN JOHANNA SCHMIDT/ZECH HERBERT, Rechte an Daten - zum Stand der Diskussion, sic! 2018, 627 et seq., 629; STEPHAN WOLF/WOLFGANG WIEGAND, in: Geiser/Wolf (eds.), Basler Kommentar Zivilgesetzbuch II, Art. 457-977 ZGB and Art. 1-61 SchIT ZGB, Basel 2023, before Art. 641 et seq. N 19c.

² BSK ZGBII-WOLF/WIEGAND, fn. 1, before Art. 641 et seq. N 5 et seq.; BARBARA GRAHAM-SIEGENTHALER, in: Aebi-Müller/Müller (eds.), Berner Kommentar, Das Eigentum - Allgemeine Bestimmungen - Art. 641-654a ZGB, Bern 2022, Zweiter Abschnitt Sachen und andere Rechtsobjekte N 243.

However, the fact that there is no such thing as “ownership rights to data” does not mean that there cannot be any **other rights to data** that would prevent the use or free dissemination of data. Such restrictions may arise in particular from copyright law, from the protection of manufacturing and trade secrets, from data protection law and, in the EU, from the so-called *sui generis* protection of databases.³

De facto control over data is also possible. Such control can arise, for example, from their storage in proprietary systems or encryption. It is also possible for a contract to stipulate that control over data is vested in one party or another. In these cases, one sometimes speaks of *data ownership*. This definition can be helpful in expressing *de facto* control. However, it should not obscure the fact that these “ownership rights” do not constitute property rights in the legal sense. Nevertheless, *de facto* control is sometimes protected by law, namely by laws protecting manufacturing and trade secrets (Art. 162 SCC and Art. 6 UCA).⁴

1.2. Copyright

Copyright protects **works of literature and art** (Art. 2 (1) Swiss Copyright Act [CopA]). These include texts, music, films, pictures, works of architecture, photographs and works with scientific content such as drawings, plans, maps or three-dimensional representations (Art. 2 (2) CopA). **Computer programs** are also deemed to be works (Art. 2 (3) CopA). **Data are not works of literature or art** and are therefore not protected as such by copyright. However, if a **literary or artistic work** is stored on a data carrier and thus **represented in data**, the copyright protection of the work also covers its representation in the form of data. Copyright law only protects works if they are **intellectual creations with individual character** (Art. 2 (1) CopA). There is an exception for photographs, which are also protected if they do not have individual character (Art. 2 (3^{bis}) CopA). In addition, **certain performances** are protected by so-called neighbouring rights. Such protection exists for performances by performing artists (Art. 33 *et seq.* CopA), e.g. musicians, actors and conductors, for producers of audio and audiovisual recordings (Art. 36 CopA), and for broadcasting organisations (Art. 37 CopA). These neighbouring rights protect the performances, sound recordings or broadcasts against their use by third parties.

The **prerequisites for protection of intellectual creations** reflect the notion that only works created by humans can be works within the meaning of copyright law.⁵ Thus, works that are created independently by computers are not protected, but works that were created by humans using computers as

³ See below, B.1.3.

⁴ See below, B.1.5.

⁵ BGE 130 III 168, E. 4.5 - “Bob Marley”; MANFRED REHBINDER/LORENZ HAAS/KAI-PETER UHLIG, in: Uhlig/Rehbinder/Haas (eds.), Orell Füssli Kommentar, CopA Urheberrechtsgesetz mit weiteren Erlassen und internationalen Abkommen, Zurich 2022 URG Art. 2 N 2; WILLI EGLOFF, in: Barrelet/Egloff (eds.), Das neue Urheberrecht, Kommentar zum Bundesgesetz über das Urheberrecht (URG) und verwandte Schutzrechte, Kommentar, Bern 2020, Art. 2 N 8; RETO M. HILTY, Urheberrecht, Bern 2020, para. 151.

tools are.⁶ Works that are generated independently by systems of so-called generative artificial intelligence (AI) on the basis of human input (through so-called prompts) are therefore not protected by copyright.⁷ The situation is different when AI is used as a tool to implement creative decisions made by humans. The boundary between the largely independent creation of works by an AI system and the use of such a system as a tool can only be determined on a case-by-case basis. The prerequisite of the **individual character** of the creation is a qualitative minimum hurdle. Only works expressing a certain degree of creativity are protected by copyright. This distinguishes protected works from banal creations and mere routine work. The individual character results from the variety of decisions made by the author and from surprising and unusual combinations, rendering it impossible for a third party to have created the same or an essentially identical work if the same task had been set for them.⁸

Computer programs are also deemed to be works (Art. 2 (3) CopA). The source code is protected by copyright if it has individual character. According to Swiss jurisprudence, this is the case if the program is new and is not banal or commonplace.⁹ However, as in the case of literary and artistic works, computer programs should also be assessed on the basis of whether it can be ruled out that a third party would have created the same or an essentially identical work if they had been given same task. However, in application, there would likely be no difference relative to the test of whether the program is banal or everyday.

Collected works are also protected by copyright if they fulfil the protection requirements of copyright law due to the selection or arrangement of the data, i.e. if they have individual character (Art. 4 (1) CopA). **Databases** are also considered collected works. Databases are thus protected if they have individual character due to the selection or arrangement of the data they contain.¹⁰ This criterion is not easily met in the case of databases. As a rule, only structured databases are protected by copyright, because unstructured databases lack an arrangement of data that could justify protection.¹¹ The selection of data in itself is unlikely to have individual character and thus justify copyright protection. Any

⁶ HILTY, Fn. 5, para. 152; ROLAND VON BÜREN, in: von Büren/David (eds.), Schweizerisches Immaterialgüter- und Wettbewerbsrecht (SIWR), II/2, Urheberrecht im EDV-Bereich, Basel 1998, para. 403.

⁷ HILTY, Fn. 5, para. 152, 184; NATHALIE TISSOT/DANIEL KRAUS/VINCENT SALVADÉ, Propriété intellectuelle, Marques, brevets, droit d'auteur, Bern 2019, para. 16.

⁸ BGE 134 III 166, E. 2.3.2 - "Arzneimittel-Kompendium"; accord: BGE 142 III 387 E. 3.1 - "Fermeture d'une Terrasse"; BGE136 III 225, E. 4.2 - "Guide orange".

⁹ URG Komm.-Egloff, fn. 5, Art. 2 N 33 with further references; OFK URG-REHBINDER/HAAS/UHLIG, fn. 5, Art. 2 N 31; WILLI EGLOFF, FAIR Works - Eckpunkte eines Urheberrechts für digitale Welt, sic! 2022, 405 et seq., 412.

¹⁰ EGLOFF, fn. 5, URG 4 N 6; HILTY, Urheberrecht, para. 249; IVAN CHERPILLOD, in: Müller/Oertli (eds.), Stämpfli's Handkommentar, Urheberrechtsgesetz (URG), Bundesgesetz über das Urheberrecht und verwandte Schutzrechte. Mit Ausblick auf EU-Recht, deutsches Recht, Staatsverträge und die internationale Rechtsentwicklung, Bern 2012, Art. 4 N 4.

¹¹ ECJ GRUR 2009, 572; OGer ZH of 1 September 1992, in: SMI 1993, 331 et seq.; URG Komm.-EGLOFF, fn. 5, Art. 4 N 6 with further references.

copyright protection of databases always relates only to the selection and arrangement of the data, i.e. to the **structure of the database**, so to speak, and not to the data as such. The individual data – and thus the entire corpus of data – are therefore not protected by copyright.

It should be noted that copyright not only protects the entire work (e.g. the entire source code), but **also parts** of it (e.g. text parts, sequences of source code or parts of a database) if those parts fulfil the criteria for protection *per se*, i.e. in particular if they have individual character (Art. 2 (4) CopA).

Copyright holders have the exclusive right to determine whether, when and how the work is used (Art. 10 (1) CopA). Part of this comprehensive right of use is the so-called **right to make available**, i.e. the right to make the work available in such a way that people can access it from places and at times of their choosing (Art. 10 (2) (c) CopA). This right covers the making available of works via the internet. Copyright-protected works may therefore only be made available as ORD with the consent of the right holder.

However, the use of copyright-protected works in research is largely permitted through **exceptions**. The use of works for personal research (e.g. writing a dissertation) is permitted through the private use exception (Art. 19 (1) (a) CopA).¹² The reproduction of works for research within an organisation can be qualified as business use and is therefore also permitted (Art. 19 (1) (c) CopA).¹³ In addition, the CopA contains an explicit exception in favour of scientific research, which allows works to be reproduced for the purpose of scientific research if the reproduction is due to the use of a technical process and the access to the works to be reproduced is lawful (Art. 24d (1) CopA). The citation of works is also permitted under the freedom to quote exception (Art. 25 CopA). If the requirements of one of these exceptions are met, works and protected performances may be used for research purposes and, in particular, reproduced, e.g. stored on a server, without the consent of the holder of the copyright and neighbouring rights. However, these exceptions do not allow works to be made accessible as ORD on a platform.

Copyright **protection is limited in time**. In the case of literary and artistic works, it ends 70 years after the death of the author, and in the case of computer programs it ends 50 years after the death of the author. For photographs with no individual character, protection ends 50 years after the photographs were created (Art. 29 et seq. CopA). The protection of performances by performers ends 70 years after the performance. The protection of producers of audio and audiovisual recordings ends 70 years after the production of the audio-visual medium. The protection of performances by broadcasting

¹² BARRELET/EGLOFF, fn. 5, Art. 19 N 11; SHK URG-Gasser, fn. 10, Art. 19 N 21.

¹³ BARRELET/EGLOFF, fn. 5, Art. 19 N 20; OFK URG-REHBINDER/HAAß/UHLIG, fn. 5, Art. 19 N 31.

organisations ends 50 years after the broadcast (Art. 39 CopA). After expiry of the protection, the works and performances enter the **public domain** and may be used freely, e.g. made available as ORD.

1.3. Sui generis rights to databases in the EU

With **Directive 96/9/EC on the legal protection of databases** (Database Directive), the then-European Community (EC) created special protection for databases in the mid-1990s. With the implementation of the Database Directive, all Member States of the EC created *copyright protection* for databases and a so-called sui generis right for the producers of databases in the national law of the Member States.¹⁴ The creation and duration of copyright protection for databases are determined by copyright law. The sui generis right arises upon completion of the making of the database, and ends after 15 years (Art. 10 (1) of the Database Directive).

Swiss law does not recognise any sui generis right, but rather only copyright protection for databases.¹⁵ Databases are thus not protected in Switzerland against extraction and/or further use of the data they contain. The sui generis right to databases must nevertheless be honoured when making research data accessible as ORD, because the data are made available worldwide (and thus also in the EU) and any form of making data publicly available is deemed reuse. Making data available as ORD can therefore infringe on the sui generis right of database creators to databases, regardless of the location of the server.

The purpose of the sui generis right to databases is to protect the investments of database authors.¹⁶ A database is a collection of works, data or other independent elements¹⁷ which are **organised systematically or methodically** and are individually accessible by electronic means or otherwise (Art. 1 (1) of the Database Directive).¹⁸ The protection thus only covers structured databases, not unstructured collections of data.¹⁹ The prerequisite for the granting of protection is that the author has made a significant investment in terms of quality or quantity in obtaining, verifying or presenting the contents of a database. However, the investment associated with the database is only considered to be the use of

¹⁴ Art. 7 et seq. Database Directive; for rationale, see in particular rec. 38 Database Directive.

¹⁵ See above, B.1.2.

¹⁶ ECJ of 9 October 2008, Case C-304/07 - Directmedia vs. Albert-Ludwigs-Universität, para. 33; ECJ of 19 December 2013, Case C-202/12, Innover vs. Wegener, para. 36-37.

¹⁷ ECJ of 29 October 2015, C-490/14 - Free State of Bavaria vs. Verlag Esterbauer GmbH, margin nos. 17 and 22.

¹⁸ According to the ECJ, it must be possible to retrieve any independent material contained within it by means "such as an index, a table of contents, or a particular plan or method of classification"; ECJ of 9 November 2004, Case C-444/2 - Fixtures Marketing vs. OPAP, para. 30.

¹⁹ ECJ of 1 March 2012, Case C-604/10, para. 30 and 32 - Football Dataco vs. Yahoo!

funds for the procurement or compilation of elements, not the investment in the creation of these elements, i.e. the data as such.²⁰

The sui generis right gives its holder the right to prohibit third parties from extracting and/or re-utilising all or a quantitatively or qualitatively substantial part of the content of a database.²¹ **Extraction** means the permanent or temporary transfer of the contents of a database to another data carrier, irrespective of the means used and the form of extraction (Art. 7 (2) (a) of the Database Directive). **Re-utilisation** means any form of making available to the public (Art. 7 (2) (b) of the Database Directive).²² A "substantial part" can be assumed if a quantitatively large part in relation to the total volume of the database is extracted and/or reutilised. A qualitatively substantial part exists if the investment made for the extracted element(s) is significant in relation to the investment in the entire database.²³ The repeated and systematic extraction and/or re-utilisation of insubstantial parts of the contents of the database imply acts which conflict with a normal exploitation of that database or which unreasonably prejudice the legitimate interests of the maker of the database is prohibited (Art. 7 (5) of the Database Directive).

While copyright law protects the selection and arrangement of data in a database, i.e. its structure²⁴, the sui generis right covers the **content of databases**, i.e. a majority of its data, by encompassing the extraction of individual or several elements from a database, irrespective of whether the structure of the database has also been copied.²⁵ The author of a database can thus prohibit third parties from extracting and re-utilising the data contained therein in any form, provided that this involves quantitatively or qualitatively substantial parts. The sui generis right conveys exclusive rights to the contents of databases and thus to certain data sets, but not to individual data contained in the database.

²⁰ ECJ of 09 November 2004, Case C-203/02 - British Horseracing vs. Hill Organization, para. 38; ECJ of 9 November 2004, Case C-444/2 - Fixtures Marketing vs. OPAP, para. 39 et seq., esp. 47; FLORENT THOUVENIN, Funktionale Systematisierung von Wettbewerbsrecht (UCA) und Immaterialgüterrecht, Diss. Zurich, Cologne/Berlin/Munich 2007, 392.

²¹ THOUVENIN, Fn. 20, 393.

²² According to the ECJ, "extraction" and "re-utilisation" include any unauthorised use of a database that impairs the investment of its maker. ECJ of 9 November 2004, Case C-203/02 - British Horseracing vs. Hill Organisation, para. 51; HEIKO SENDROWSKI, Zum Schutzrecht "sui generis" an Datenbanken, GRUR 2005, 369 et seq., 374.

²³ ECJ of 5 March 2009, Case C-545/07 - Apis-Hristovich vs. Lakorda, para. 56 et seq., esp. 59, 66 and 74; SENDROWSKI, fn. 22, 375; ANDREAS WIEBE, Schutz von Maschinendaten durch das sui-generis-Schutzrecht für Datenbanken, GRUR 2017, 338 et seq., 343 et seq.

²⁴ Rec. 15 and 39 Database Directive.

²⁵ See also Rec. 58 Database Directive, according to which copyright law protects the structure, whereas the *sui generis right* protects the content; ECJ of 5 March 2009, Case C-545/07 - Apis-Hristovich vs. Lakorda, para. 55.

1.4. Direct taking over of work products (Art. 5 (c) UCA)

The UCA not only provides for the protection of manufacturing and trade secrets, but also protects work product by making it an offence to directly take over the work product of another. According to Art. 5 (c) UCA, persons act unfairly if they take over and exploit another person's work product that is ready for the market by means of technical reproduction processes without any reasonable effort of their own. The elements of this also covers the direct transfer of data and can therefore have a similar effect to that provided under the sui generis right to databases.²⁶

According to legal scholarship and case law, **work product ready for the market** is a product that can be commercially utilised without further action.²⁷ This work product must be materialised in some form, because otherwise it could not be adopted by a technical reproduction process.²⁸ This includes not only physical but also non-physical work products, e.g. audio and audiovisual recordings, computer programs or data stored on a data carrier.²⁹ The constituent element of the **technical reproduction process** has not been defined in more detail either by the legislature or by legal scholarship and jurisprudence. However, digital reproduction processes, e.g. *web scraping* or the creation of digital copies of data,³⁰ must undoubtedly be qualified as technical reproduction processes. Adoption of a work by which the work product is concretely included in the reproduction process is deemed to constitute **taking over**,³¹ and any commercial application or professional use in commercial competition is deemed to constitute **utilisation**.³² This primarily refers to utilisation of the adopted work product for manufacturing a competing product. However, according to some legal scholarship and case law, it is sufficient for the party taking over the work product to use it as the basis for his own work.³³

The legislator has deliberately left open the criterion of what constitutes "**own reasonable expenditure**". It should permit "weighing of the unjustified competitive advantage of the second competitor" and allow account to be taken of the amortisation of "the costs incurred by the first competitor in creating

²⁶ See above, B.1.3.

²⁷ FLORENT THOUVENIN, Art. 5 (c) UCA - reloaded, sic! 2018, 595 et seq., 598; BGE 131 III 384, 389 - "Suchspider".

²⁸ BGE 131 III 384, 389- "Suchspider"; similarly ROLF H. WEBER/LENNART CHROBAK, in: Heizmann/Loacker (eds.), Kommentar zum Bundesgesetz gegen den unlauteren Wettbewerb (UWG), Zurich/St. Gallen 2018, Art. 5 (c) N 19.

²⁹ BGE 131 III 384, 389-390. - "Suchspider"; UCA-Komm.-WEBER/CHROBAK, fn. 28, Art. 5 (c) N 15, 18; SIMONE BRAUCHBAR BIRKHÄUSER, in: Jung (ed.), Stämpflis Handkommentar, Bundesgesetz gegen den unlauteren Wettbewerb, Bern 2023, Art. 5 N 23; RETO ARPAGAU, in: Hilty/Arpagaus (eds.), Basler Kommentar, Bundesgesetz gegen den unlauteren Wettbewerb (UWG), Basel 2013, Art. 5 N 31, 36.

³⁰ UWG KommWEBER/CHROBAK fn. 28, 5 N 43; BSK UWG-ARPAGAU, fn. 29, 5 N 84; thus probably also SHK UWG-BRAUCHBAR BIRKHÄUSER, fn. 29, Art. 5 N 33.

³¹ UWG Komm.-WEBER/CHROBAK, fn. 28, Art. 5 (c) N 23; ARNAUD Nussbaumer, in: Martenet/Pichonnaz (eds.), Commentaire Romand, Loi contre la concurrence déloyale (LCD), Basel 2017, Art. 5 N 68.

³² UWG KommWEBER/CHROBAK fn. 28, Art. 5 (c) N 25.

³³ BSK UWG-ARPAGAU, Fn. 29, Art. 5 N 74.

the adopted product".³⁴ It is generally recognised that reasonable expenditure is to be determined by way of a so-called "double expense comparison".³⁵

Whether the requirements of Art. 5 (c) UCA are met can only be determined on a case-by-case basis. However, the provision shows that the taking over of third-party data can even constitute a breach under the UCA where the data are not kept secret and are generally accessible.

1.5. Protection of manufacturing and trade secrecy (know-how / proprietary information)

Although there are no intellectual property rights to manufacturing and trade secrets, there are several legal provisions which protect secrets against disclosure and use by third parties. Those provisions impose sanctions for **interference with the de facto control over data** in certain circumstances and thus serve to legally safeguard actual control over data.³⁶ The provisions of Art. 6 UCA and Art. 162 SCC are foremost among these.

Pursuant to Art. 6 UCA, persons act unfairly (and therefore unlawfully) if they exploit or disclose to others manufacturing or trade secrets that they have found out (through espionage) or obtained by other unlawful means. A **secret** is "special knowledge of facts that are not in the public domain or generally accessible, which the manufacturer or owner of the secret has a legitimate interest in keeping secret and which the manufacturer or owner actually wants to keep secret".³⁷ A secret of this kind must also have a potential impact on the company's business results, i.e. it must be "relevant to production or business" in order to be covered by the protection of Art. 6 UCA.³⁸

However, **Art. 6 UCA** does not protect company secrets per se, but only grants parties the right to assert claims against the **utilisation or disclosure of secrets** by others after they have been found out by commercial espionage or unlawfully obtained by other means.³⁹ After such unauthorised knowledge has been obtained, Art. 6 UCA additionally requires an act that is objectively capable of impacting competition.⁴⁰ If these requirements are met, the party with an entitlement to do so can assert the statutory claim for injunctive relief and redress (Art. 9 (1) (a) and (b) UCA). In addition, Art. 23 (1)

³⁴ Dispatch on the UCA bBl 1983 1009, 1071.

³⁵ BGE 131 III 384, E. 4.3 - "Suchspider"; BGE 134 III 166, E. 4.3 - "Arzneimittelkompendium"; BGE 139 IV 17, E. 1.5 - "Cardsharing"; BSK UWG-ARPAGAU, fn. 29, Art. 5 N 91; UCA KommWEBER/CHROBAK fn. 28, Art. 5 (c) N 47, 53.

³⁶ ALFRED FRÜH, Datenzuordnung und Datennutzung, digma 2019, 172 et seq., 173.

³⁷ BSK UWG-FRICK, fn. 29, Art. 6 N 12; BGer 4A_78/2014 of 23 September 2014, E. 11.1; OGer ZH UE140269 of 19 March 2015, E. 2.c.

³⁸ SHK UWG-MABILLARD, fn. 29, Art. 6 N 13; BSK UWG-FRICK, fn. 29, Art. 6 N 15, in each case with further references.

³⁹ BSK UWG-FRICK, fn. 29, Art. 6 N 5; SHK UWG-MABILLARD, Art. 6 N 21.

⁴⁰ SHK UWG-MABILLARD, Art. 6 N 21; BSK UWG-FRICK art. 6 N 53, each with further references.

of the UCA makes a violation of Art. 6 of the UCA punishable by custodial sentence or monetary penalty upon complaint.

Under **Art. 162 of the Swiss Criminal Code**, anyone who betrays a manufacturing or trade secret that while under a statutory or contractual duty contract not to reveal it, or exploits such a betrayal for personal or third-party benefit, is liable to a custodial sentence not exceeding three years or a monetary penalty. With the exception of the **contractual or statutory duty of confidentiality** required under this section of the Criminal Code, the offence under criminal law is largely identical to that under Art. 6 UCA.⁴¹ In particular, the concept of manufacturing and trade secrets in Art. 6 UCA corresponds to that in Art. 162 SCC.⁴²

The protection of manufacturing and trade secrets under Art. 6 UCA and Art. 162 SCC is not limited in time, so that it can (theoretically) last forever. However, the **protection ends** as soon as **the information is no longer secret**.⁴³

It is unclear whether **research data** is protected under Art. 6 UCA and Art. 162 SCC if it is kept secret. As explained above, in order to qualify as a manufacturing or trade secret, the secret facts must potentially have a certain **commercial value** or the secret facts must potentially have an impact on the company's results.⁴⁴ Against this background, scholars have argued that information of scientific, academic value is not a secret within the meaning of Art. 6 UCA (and thus within the meaning of Art. 162 SCC) as long as it is not transferred to a business entity.⁴⁵ Other authors do mention research and development work (university or in-house) as examples of manufacturing or trade secrets, but also make the proviso that such work must be important for business success and thus have a certain commercial relevance.⁴⁶ Commercial value is likely to be found present if, as part of their private-sector activities (contract research for companies, preparation of expert reports, etc.), universities generate research data. According to current legal scholarship and case law, it is uncertain whether research data created in the course of "normal" and therefore fundamentally non-commercial university research has

⁴¹ MARCEL ALEXANDER NIGGLI/NADINE HAGENSTEIN, in: Niggli/Wiprächtiger (ed.), Basler Kommentar, Strafgesetzbuch und Jugendstrafgesetzbuch (StGB/JStGB), Basel 2019, Art. 162 N 52; SHK UWG-Mabillard, fn. 38, Art. 6 N 5 with further references.

⁴² SHKUWG-MABILLARD, fn. 38, Art. 6 N 8; BSKUWG-FRICK, fn. 29, Art. 6 N 13; LORENZA FERRARI HOFER/DAVID VASELLA, in: Amstutz/Atamer (eds.), Handkommentar zum Schweizer Privatrecht, Wirtschaftliche Nebenerlasse: FusG, UCA, KKG, PauRG and PrHG, Zurich 2023, Art. 6 N 3.

⁴³ SHK UWG-MABILLARD fn. 38, Art. 6 N 19; BSK UWG-FRICK, fn. 29, Art. 6 N 51.

⁴⁴ On the SCC: ANDREAS DONATSCH, in: Orell Füssli Kommentar StGB/JStGB, Mit weiteren Erlassen und Kommentar zu den Strafbestimmungen des SVG, BetrG, AIG und OBG, Zurich 2022, Art. 162 N 3; BSK StGB-Niggli/Hagenstein, fn. 41, Art. 162 N 9; STEPHAN SCHLEGEL, in: Wohlers/Godenzi/Schlegel (eds.), Handkommentar, Schweizerisches Strafgesetzbuch, Bern 2020, Art. 162 N 3.

⁴⁵ BSK UWG-FRICK, fn. 29, Art. 6 N 15.

⁴⁶ OFK StGB-DONATSCH fn. 44, Art. 162 N 3.

commercial value within the meaning of Art. 6 UCA and Art. 162 SCC, and is therefore subject to the protection of secrets under these provisions.

However, an interpretation based on the meaning and purpose of the UCA would militate in favour of **subjecting research data to the protections of Art. 6 UCA and Art. 162 SCC**. The purpose of these provisions is to prevent economic losses due to the unauthorised disclosure and exploitation of secrets. The confidentiality of university research data is also geared towards such protective measures, which are intended to enable the university or its researchers to control crucial work product and to prevent third parties (e.g. companies or other researchers) from gaining commercial (or other) advantages through the use of the research data. Against this background, it is obvious that university research data should be classified as trade secrets.

Research data can thus be qualified as **secrets within the meaning of Art. 6 UCA and Art. 162 SCC**. However, this does not mean that making research data available as ORD fulfils the requirements of these provisions. **Art. 6 UCA** only covers the utilisation or disclosure of secrets that the person in question has found out (through espionage) or otherwise unlawfully obtained. This is not usually the case when making research data available as ORD, because the researchers have access to the data as part of their research work or have generated the data themselves. A different rule will only apply if researchers have obtained access to the data by unauthorised means. However, a violation of **Art. 162 SCC** is possible. This presupposes that there is a **legal or contractual obligation** to keep information secret. Making research data available as ORD may be obstructed by confidentiality obligations arising in particular from contracts concluded with companies (or other research institutions) as part of research collaborations.⁴⁷ Such contracts are often concluded in advance of the actual collaboration, e.g. in the form of non-disclosure agreements (NDA) or material transfer agreements (MTA). These contracts are very important in practice. For research collaborations with companies (or other research institutions), it is essential that the parties comply with the terms of these contracts, including not only, but in particular, the provisions on confidentiality. If the data are made accessible as ORD contrary to a contractual duty of confidentiality, this is not only a breach of contract, but also a violation of Art. 162 SCC and therefore a criminal offence. This offence is punishable upon complaint by a custodial sentence of up to three years or a monetary penalty. The person authorised to file the complaint is the party with rights to the confidential information.⁴⁸

Other criminal offences aimed at protecting secrets can be found in Swiss law under criminal offences involving breaches of official and professional duties, namely the violation of **official secrecy** (Art. 320 SCC). The concept of secrecy is similar to that of Art. 6 UCA and Art. 162 SCC. Pursuant to Art. 320

⁴⁷ See below, C.4.

⁴⁸ BSK StGB-NIGGLI/HAGENSTEIN, fn. 41, Art. 162 N 56-57; OFKStGB-DONATSCH, fn. 44, Art. 162 N 8.

SCC, all information that is not generally known or accessible which the person holding rights to the information wishes to protect from disclosure and in whose secrecy there is an objective interest is also deemed to be a secret.⁴⁹ A secret becomes an official secret if the fact to be kept secret has been confided to the public official in his or her capacity as a public official or if he or she has gained knowledge of it due to his or her official position.⁵⁰ In other words, there must be a causal link between the disclosure of the secret and the official function. As far as one can see, the question of whether **university research data** fulfils this criterion has not yet been discussed in legal scholarship and/or case law. Consequently, the legal provision requires interpretation. The wording of Art. 320 SCC ("confided" and "come to his knowledge") indicates that only secret facts that already exist and of which the public official gains knowledge in the course of his or her official duties are covered. However, findings or facts that are produced or generated in the course of official activities are not included. Research data generated as part of university research is therefore not covered by the concept of official secrecy. This result is also supported by an interpretation of the meaning and purpose of the provision, which primarily serves to protect secrets in which there is a public interest (e.g. keeping Switzerland's foreign policy strategy secret) or an individual interest (e.g. criminal record entries) and which have been kept in an official capacity. Even if there are constellations in which there are public or private interests in the confidentiality of research data, the confidentiality of research data does not (primarily) serve to protect the interests of third parties, but rather to protect the interests of researchers and research institutions in controlling the data generated in the course of their research, and in the scientific or commercial utilisation of that data. The research data generated by public research institutions – e.g. the institutions within the ETH Domain – as part of their research are therefore trade/business secrets (in a broader sense) and not official secrets.

2. Rightsholder status

Insofar as rights to data exist, the question arises as to who is entitled to these rights. Intellectual property law only governs the question of original acquisition and clarifies that intellectual property rights can be transferred, i.e. also acquired derivatively. However, these statutes (with the exception of Art. 17 CopA) do not govern who is entitled to the rights to intellectual property as between employer and employee. In private-law employment relationships, this question is dealt with for patent and design law by Art. 332 Swiss Code of Obligations (CO); in the case of copyright law, the legislator has deliberately not enacted provisions covering the question (except for computer programs in Art. 17 CopA). In

⁴⁹ BSK StGB-OBERHOLZER fn. 41, Art. 320 N 8; OFK StGB-ISENRING fn. 44, Art. 320 N 3, in each case with further references.

⁵⁰ Cases: SUVA patient file (BGE 142 IV 65, E. 5.2); all information in connection with criminal proceedings (BGer 6B_439/2016 of 21 April 2017, E. 2.2.2); entries in criminal records (BGE 127 IV 122, E. 1).

relations between researchers and the institutions within the ETH Domain, the issue is governed by Art. 36 of the ETH Act.

Art. 36 (1) ETH Act reads: "With the exception of copyright, all other rights to intellectual property created during the official duties of persons in an employment relationship as defined in Article 17 shall belong to the two federal institutes of technology and the four research institutes within the ETH Domain."

The wording of the law and the explanations in the dispatch make clear that the provision covers all intellectual property covered by special legislation, i.e. in particular inventions, literary and artistic works, designs, trademarks, topographies of semiconductor products and plant varieties.⁵¹ Neither the Act nor the dispatch comment on rights to data that are not protected by intellectual property rights. The question of rights to trade secrets, which is at the forefront where data are concerned, is also not directly addressed. However, the dispatch makes it clear that "commercially exploitable know-how is created on a large scale" at the institutions within the ETH Domain, and that the aim of the revision of Art. 36 of the ETH Act is "a clear allocation of rights to all intellectual property in the ETH Domain".

As explained above, **data are** not tangible assets,⁵² but rather **intellectual property**.⁵³ Art. 36 of the ETH Act stipulates that the institutions within the ETH Domain own **"all rights to intellectual property"** created by employees of these institutions in the course of their official duties, with the exception of copyrights. The marginal note in Art. 36 of the ETH Act also uses the term "intellectual property" rather than "intellectual property rights". The wording of the provision thus speaks in favour of a comprehensive scope of application that covers all intellectual property, not just the intellectual property rights provided for by special legislation, and thus also includes rights to data, where such exist.

An interpretation based on the meaning and purpose of the provision leads to the same result, especially since the Federal Council, according to the dispatch, wanted to establish **"a clear allocation of rights to all intellectual property in the ETH Domain"**. In the case of tangible assets, the fact that the employer is entitled to the goods that its employees create in the course of their work is so self-evident that the issue is not even expressly set out in labour law. An express legal provision only exists for intellectual property rights - and there the question is resolved by allocating the rights to the employer, except for copyright, which is dominated by the so-called creator principle. Even in copyright law, the sole express legal provision provides for allocation of rights to the employer, and only applies to

⁵¹ Dispatch on ETH Act, BBl 2002 3465 et seq., 3495.

⁵² See above, B.1.1.

⁵³ FLORENT THOUVENIN, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, SJZ 113/2017, 21 et seq., 25.

computer programs (Art. 17 CopA). The same applies to the institutions within the ETH Domain pursuant to Art. 36 (2) sentence 1 of the ETH Act.

As explained above, data are only partially and indirectly protected by intellectual property rights governed by specific legislation.⁵⁴ However, data are covered by the **protection of manufacturing and trade secrets provided for** in Art. 6 UCA and Art. 162 SCC if they meet the prerequisites to be qualified as secret.⁵⁵ The protection of manufacturing and trade secrets also confers **rights to the confidential information**. Like intellectual property rights, these are to be categorised as subjective rights.⁵⁶ In the Common Law, the protection of *trade secrets* is understood as an intellectual property right.⁵⁷ This understanding is also the basis of the TRIPS Agreement, which Switzerland has also signed and ratified.⁵⁸ There are therefore perfectly valid reasons for categorising the rights to secret information which the protection of manufacturing and trade secrets confers on the persons holding rights to the secrets as intellectual property rights, especially since these are subjective rights to intangible assets. Whether these reasons are persuasive under Swiss law can be left open here, because data are undoubtedly intellectual property within the meaning of Art. 36 of the ETH Act. The rights to data are thus covered by this provision and the legal rights to the data are assigned to the institutions within the ETH Domain.

An interpretation of Art. 36 of the ETH Act thus leads to the conclusion that the **rights to data** created by the employees of the institutions within the ETH Domain in the performance of their official duties belong to those institutions.

3. Data protection law

The Data Protection Act (Federal Act on Data Protection, *FADP*) governs the processing of **personal data of natural persons** (Art. 2 (1) FADP). Personal data is defined as all information relating to an identified or identifiable natural person (Art. 5 (a) FADP). The concept of personal data is therefore extremely broad. The concept of **processing** is also extremely broad. It covers all handling of personal data, including in particular the collection, storage, retention, use, modification, disclosure, publication,

⁵⁴ See above, B.1.2.

⁵⁵ See above, B.1.5.

⁵⁶ THOUVENIN, Fn. 20, 560 et seq.; SHK UWG-Mabillard, Fn. 29, Art. 6 N 1 with further references.

⁵⁷ OHLY ANSGAR, Harmonising the Protection of Trade Secrets: Challenges and Perspectives, in: Werra (ed.), *La protection des secrets d'affaires / The Protection of Trade Secrets*, Zurich 2013, 32; MARCO BRONCKERS/NATHALIE M. McNELIS, Is the EU obliged to improve the protection of trade secrets? An inquiry into TRIPS, the European Convention on Human Rights and the EU Charter of Fundamental Rights, *EIPR* 2012, 673 et seq., 677.

⁵⁸ OHLY ANSGAR, Harmonising the Protection of Trade Secrets: Challenges and Perspectives, in: Werra (ed.), *La protection des secrets d'affaires / The Protection of Trade Secrets*, Zurich 2013, 33; INGO MEITINGER, Die globale Rahmenordnung für den Schutz von Geschäftsgeheimnissen im TRIPS-Abkommen der WTO und ihre Auswirkungen auf die Rechtslage in der Schweiz, *sic!* 2002, 145 et seq., 147.

archiving, erasure and destruction of data (Art. 5 (d) FADP). The FADP therefore has an extremely broad scope of application and also covers a host of research data made accessible as ORD on the internet.

The processing of **anonymised data and factual data** (e.g. data on the wear and tear of an aircraft turbine), which have no personal reference from the outset, are not covered. Anonymisation involves changing personal data to such an extent that it can no longer be linked to a specific person, or only with a disproportionate amount of effort.⁵⁹ However, it is still not sufficiently clear when personal data is considered anonymised. In particular, it is unclear at what level of abstraction re-identification appears to be disproportionately complex. In addition, from a technical perspective, the extent to which anonymisation is even feasible is controversial. Developments in the field of AI and big data in particular are making it ever easier to draw conclusions from supposedly anonymised data records about identified or identifiable persons.

As federal bodies, the institutions within the ETH Domain may only process personal data if there is a **legal basis** for doing so. This is the case here. Pursuant to Art. 36c (1) of the ETH Act, the ETH and the research institutes may process personal data, including sensitive personal data, insofar as this is required for a given project. When processing personal data, the institutions within the ETH Domain must comply with the provisions of the FADP. This is explicitly mentioned in Art. 36c (2) ETH Act, but already follows from the FADP, because the institutions within the ETH Domain are qualified as federal bodies under data protection law (Art. 2 (1) (b) in conjunction with Art. 5 (i) FADP).

According to Art. 39 FADP, federal bodies may process personal data for **non-personal purposes**, in particular for research, planning or statistics if four conditions are met: (i) the data are anonymised as soon as the purpose of processing permits; (ii) the federal body only discloses sensitive personal data to private persons in such a manner that the data subjects are not identifiable; (iii) the recipient only transmits the data to third parties with the consent of the federal body that disclosed the data; and (iv) the results are only published in such a manner that the data subjects are not identifiable. These requirements also apply to research at the institutions within the ETH Domain. Art. 36c (1) of the ETH Act merely forms the legal basis that is required *to enable* these institutions to be authorised to process personal data in the context of research; Art. 39 FADP contains specific provisions on *how* the processing must be carried out.

Although the requirements of Art. 39 FADP are aimed at the publication of research results in scientific publications, they also apply to the **publication of research data**. The requirement of anonymisation

⁵⁹ BEAT RUDIN, in: Baeriswyl/Pärli/Blonski (eds.), Stämpfli's Handkommentar, Datenschutzgesetz (DSG), Bern 2021, Art. 5 N 13; GaborP. BLECHTA/LUCA DAL MOLIN/KIRSTEN WESIACK-SCHMIDT, in: Blechta/Vasella (eds.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz (DSG/BGÖ), Basel 2024, Art. 5 N 35.

is mentioned twice in Art. 39 FADP: in respect of processing the data in (i) and in respect of publishing the results in (iv). This makes it clear that (i) personal data must be anonymised as soon as possible when processed for research purposes and (ii) may only be published in anonymised form. **Personal data may therefore only be made accessible in anonymised form as ORD.**

C. RESTRICTIONS ON ORD

1. Question presented and approach taken

When making research data accessible as ORD, the requirements of the applicable (objective) law must be complied with and it must be ascertained whether third parties can assert (subjective) rights (e.g. copyrights or contract claims) that prevent research data from being made accessible as ORD.

Under the heading “**legal restrictions**”, we analyse whether federal law contains legal provisions that prevent research data from being made accessible as ORD. In order to answer this very broad question, the first step was to determine which federal laws might contain norms that prevent the ETH Domain institutions from making research data accessible. The selection of potentially relevant enactments was defined by the regulatory scope of the respective federal laws and the areas of activity of the institutions within the ETH Domain. At several meetings with representatives of all of the institutions within the ETH Domain, the list of potentially relevant enactments was reviewed for relevance and for any gaps in the law. No additional areas of legislation were identified that would also need to be analysed.

However, in view of the **comprehensive nature of the question**, it can be assumed that federal law does contain further provisions that prevent research data from being made accessible as ORD, provisions which could not be identified by our approach and were therefore not taken into account in this report. The researchers and/or the legal departments of the institutions within the ETH Domain will therefore **have to check for each specific data set whether there are any provisions that prevent the data from being made accessible**. It should generally be possible to assess this specific question because the researchers and/or the legal departments of the respective institutions will be familiar with the standards relevant to their specific research area.

Based on the procedure outlined above, the following regulatory areas were identified and analysed: export control law, information security law, health law, genetic engineering law, environmental law, chemicals law, food law, energy and nuclear energy law, animal welfare law and financial markets law. As noted, it can be assumed that there are other areas of legislation that contain provisions that prevent research data from being made accessible as ORD. The following explanations should therefore **not be understood as an exhaustive listing of all legal restrictions applicable to ORD**.

Under the heading "**rights of third parties**", we examine which (subjective) rights of third parties and which contractual obligations may prevent the publication and reuse of research data as ORD.

2. Legal restrictions

2.1. Export control

Export restrictions may apply to research data. According to the Goods Control Act (GCA)⁶⁰, in addition to physical goods, goods also include software and technologies, i.e. information for the development, manufacture or use of goods that is neither generally accessible nor serves the purposes of pure scientific research (Art. 3 (d) GCA).

Research institutions must comply with export control regulations⁶¹. The export of research data may require authorisation in individual cases or may be completely prohibited. Whether such restrictions apply depends on the content of the research data and the destination country. If research data is made available as ORD, export control is particularly difficult because the transfer cannot be physically controlled at borders, and the data are generally made accessible worldwide.

If the research data contain information on the production of sensitive goods, their export will always require authorisation. According to Art. 3 (b) GCA, sensitive data include not only data from defence technology, but also numerous seemingly harmless data, provided that they can also be used for military purposes (dual-use goods). Dual-use goods and the parameters for their qualification are listed in the list of dual-use goods contained in Annexes 1 and 2 of the Goods Control Ordinance (GCO).⁶² In essence, these are dual-use goods that were originally designed for civilian use but can, due to their characteristics, also be used for military purposes. Examples include information from the fields of telecommunications, electronics, chemistry, marine technology and encryption technology. A key characteristic of dual-use goods – in contrast to special military goods or war material – is that their area of application or end use is often unclear. Annex 3 GCO lists what is necessary for military deployment, e.g. information on the production of chemical or biological agents, associated equipment or the use of radioactive substances.

⁶⁰ Federal Act on the Control of Goods for Civilian and Military Use, Special Military Goods and Strategic Goods, SR 946.202.

⁶¹ In Switzerland, a number of enactments apply in connection with export controls, namely the Goods Control Act (GCA), the Goods Control Ordinance (GCO), the Ordinance on the Export and Brokerage of Goods for Internet and Mobile Telecommunications Surveillance (VIM), the Embargo Act (EmbA), the War Material Act (WMA) and the relevant goods lists. There are also international agreements: The Arms Trade Treaty (ATT); the Wassenaar Arrangement (EWA); the Chemical Weapons Convention (CWC).

⁶² Ordinance on the Control of Goods for Civilian and Military Use, Special Military Goods and Strategic Goods, SR 946.202.1.

The GCA applies to the export of research data that is not yet publicly accessible. It is not applicable to the export of research data that is already generally known and accessible. Information sources are generally accessible if they are technically suited and intended to provide information to the general public. In the case of research data, this means in particular that data that has already been published or is generally known (e.g. in a scientific publication) is not subject to export control restrictions and can therefore be published as ORD.

The export control restrictions do not apply to information from basic scientific research. According to Annex 1 GCO, basic research is "[...] experimental or theoretical work primarily aimed at gaining new knowledge about fundamental principles of phenomena or facts that are not primarily directed towards a specific practical goal or purpose".

The way in which technology and software are exported is irrelevant from the perspective of the GCA. In order to trigger the legal consequences of the GCA, it is sufficient for the goods to reach the customer abroad. The terms export and transit therefore also cover non-physical transmission, e.g. via data lines. The question of what rule applies if the data are not exported but made available for download on a server located in Switzerland remains unresolved. At least if access to the research data is via repositories and the recipients have to register before downloading the data, it is possible to trace the destination country to which the research data are sent and prevent export to certain countries. However, misuse by circumventing the registration process cannot be ruled out. The security and control mechanisms required when making research data accessible as ORD via repositories have not yet been analysed in detail from a legal perspective and are unclear.

It is thus clear that research data that are to be published as ORD must be checked in accordance with export control regulations to determine whether they contain information or software that requires authorisation or is prohibited.

The examination must be carried out on a case-by-case basis for the specific data. Research data containing information prohibited under the GCA may not be made accessible as ORD. In order for research data subject to authorisation to be published as ORD, an export licence must be obtained for all countries if unrestricted access to ORD is to be possible from all countries.

Consequently, the publication of research data as ORD is prohibited if such data qualify as dual-use goods. The qualification of research data as dual-use goods is based on the list of dual-use goods in Annexes 1 and 2 of the GCO.

2.2. Information security law

Research data may contain information that is considered sensitive by the state. Such information may fall under the Information Security Act (ISA), which restricts its use as ORD.

The purpose of the ISA is to ensure the secure processing of information for which the federal government is responsible and the secure use of federal IT resources (Art. 1 (1) ISA). The ISA serves to protect various public interests, such as the authorities' ability to make decisions and take action, as well as Switzerland's internal and external security (Art. 1 (2) ISA). The ISA imposes obligations *inter alia* on the federal administration, which also includes the decentralised administrative units in accordance with their organisational enactments.⁶³ The institutions within the ETH Domain are decentralised administrative units and are therefore covered by the ISA (see Appendix 1: list of administrative units of the Federal Administration, B., VI., points 2.2.5-2.2.10 of the Government and Administration Organisation Ordinance).

The ISA stipulates that the Federal Council may restrict the application of the law to those decentralised federal administration organisations that carry out security-sensitive activities or that use or access federal IT resources to carry out their tasks (Art. 2 para. 3 ISA). The Federal Council has made use of this option in the Information Security Ordinance (ISO) and at the same time clarified in Art. 2 para. 2 ISO which provisions of the ISA apply to these decentralised units of the Federal Administration. In a letter dated 17 December 2024, the Federal Department of Economic Affairs, Education and Research (EAER) confirmed that none of the EAER's decentralised units – and thus none of the institutions of the ETH Domain – are constantly engaged in security-sensitive activities. The institutions of the ETH Domain are therefore not fully subject to the ISA. However, the ISA does apply when institutions of the ETH Domain process classified federal information or use or access federal IT resources (Art. 2 para. 3 ISA in conjunction with Art. 2 para. 2 ISO).

Pursuant to the ISA, information is classified as "internal" if its disclosure to unauthorised persons "may prejudice" the public interest (see Art. 13 (1) ISA). Information is classified as "confidential" if its disclosure to unauthorised persons could "significantly impair" the public interest (see Art. 13 (2) ISA). Information must be classified as "secret" if its disclosure to unauthorised persons could "seriously harm" the public interest (see Art. 13 (3) ISA). If information does not fulfil the criteria under Art. 13 ISA, it is not classified and is not subject to any special legal requirements in Switzerland, unless it is personal data or specific provisions apply (such as for official secrets). However, if the information in question is classified, it is not freely accessible. Access is only granted to persons who can guarantee that they handle the information appropriately and need it to fulfil a legal task and, if applicable, have a contractually agreed access authorisation (Art. 14 (1) (a) ISA). This may make it impossible to use such information as ORD.

⁶³ See, Dispatch on the Federal Act on Information Security of 22 February 2017, BBl 2017 2953 et seq., 3012. See also Art. 2 (3) of the Government and Administration Organisation Act (GAOA), which explicitly states this.

The requirements for the ETH Domain and other decentralised administrative units are specified in the implementing provisions of the Information Security Ordinance (ISO). The basic principle is that the disclosure and making available of classified information must be kept to a minimum (Art. 16 (1) ISO). The individual administrative units also regularly issue directives (e.g. the ETH's Research Data Management Guidelines) in which they define their own information security requirements and specifications tailored to their area.⁶⁴

Since classified information may by definition be available only to a limited group of persons, it is prohibited to make such information accessible as ORD.

2.3. Health law

2.3.1. General remarks

Healthcare data is heavily regulated in Switzerland. Sensitive data – often personal data – is the rule rather than the exception in this sector. Data subjects are particularly vulnerable, especially if their bodies are interfered with in order to collect data, (e.g. when taking blood samples). In addition, information between doctors or researchers and patients is asymmetric, and that is very difficult to resolve.

Medical professionals and their assistants are therefore subject to duties of professional secrecy under criminal law (Art. 321 Swiss Criminal Code [SCC]), which prohibits them from disclosing professional secrets without the patient's consent. The violation of professional secrecy in human research is also punishable by law (Art. 321^{bis} SCC). *Informed consent* is the prevailing principle in healthcare law. As healthcare in Switzerland is primarily a cantonal matter, the classic realm of medical care is subject to cantonal law (e.g. cantonal healthcare laws). Therefore no further comments on legal issues relating to medical care will be addressed here.

2.3.2. The area of human research

In many areas, research relies heavily on the use of data from the healthcare sector. Art. 118b of the Federal Constitution therefore empowers the federal government to issue regulations on research involving human beings "where this is required in order to protect their dignity and privacy" (para. 1, sentence 1). In this context, the Federal Government must preserve the freedom to conduct research, and must take into account the importance of research for health and society (para. 1, sentence 2).

On this basis, the federal government has enacted the **Human Research Act (HRA)**. This applies to all "research on human diseases and on the structure and function of the human body", including when

⁶⁴ ETH Zurich has done so, for example, in its directive "Information Security at ETH Zurich" of 9 April 2018.

biological material or health-related personal data is used (Art. 2 (1) (d) and (e) HRA). In addition to all medical research,⁶⁵ this term can also include research into the prevention of accidents or sports injuries, research in health psychology, as well as social science and humanities research that deals with the connection between social conditions and specific diseases, or the social impact of diseases.⁶⁶ The HRA also applies to clinical trials with therapeutic products (Art. 53 Therapeutic Products Act). Whether the HRA applies must be examined on a case-by-case basis.

In the context of ORD, the special rules applicable to health-related personal data are relevant. The HRA governs not only the collection of data, for example in the context of research projects with individuals (in the form of surveys or observations), but also their secondary use (i.e. the **further use** of such data). The expression "further use" is construed very broadly and covers any handling for research purposes of biological material that has already been extracted, and any handling of data that have already been collected (Art. 24 Human Research Ordinance [HRO]).⁶⁷

The HRA distinguishes between the further use of biological material and genetic data (Art. 32 HRA), on the one hand, and non-genetic health-related personal data on the other (Art. 33 HRA). Depending on the category, different requirements apply to their further use, which are briefly outlined below.

Biological material and genetic data may be used further in *unencrypted* form for a research project in accordance with Art. 32 (1) HRA if the person concerned has given informed consent. However, if the material and data are *encrypted* (pseudonymised), i.e. linked to a specific person via a key (see Art. 3 (h) HRA), and can therefore only be identified by those persons who can decrypt the encrypted information, further use *for research purposes is generally* permitted if the data subject has given informed consent (Art. 32 (2) HRA; so-called general consent). If biological material and genetic data are to be *anonymised* and then *generally reused for research purposes*, the person concerned must be informed in advance and must not have dissented to the anonymisation (Art. 32 (3) HRA).⁶⁸

In the case of non-genetic health-related data, the possibilities for further use are more extensive. Such data may *generally* continue to be used in *unencrypted* form *for research purposes* if the data subject

⁶⁵ Accord BENEDIKT VAN SPYK, in: Rütsche (ed.), Stämpfli Handkommentar, Humanforschungsgesetz (HFG), Bundesgesetz vom 30. September 2011 über die Forschung am Menschen, Bern 2015, Art. 3 N 16 such as with the physical and psychiatric causes of illness (basic research); translation of basic knowledge to the clinical sector (translational research); the development, progression, diagnosis, prevention and treatment of diseases (clinical research); the frequency and distribution of diseases in society (epidemiological research).

⁶⁶ SHK HFG-VanSPYK, Fn 65, Art. 3 N 19.

⁶⁷ The Ordinance explicitly mentions the procurement, compilation or collection, registration or cataloguing, storage or recording in biobanks or databases, as well as the making available, provision or transmission of biological material or health-related personal data.

⁶⁸ As to this entire subject area, see: SAMUEL MÄTZLER, Datenschutz in der (Human-)Forschung: Grundlagen und Probleme bei der Sekundärnutzung von Personendaten, in: Jusletter of 30 January 2023, para. 44.

has given informed consent (Art. 33 (1) HRA; general consent). If the data are *encrypted*, further use *for research purposes* is *generally* permitted, provided the data subject has been informed in advance and has not dissented (Art. 33 (2) HRA).⁶⁹

The further use of anonymously collected and anonymised health-related data does not fall within the scope of the HRA and is therefore permitted without conditions.⁷⁰ However, this only relates to the further use of data that have already been collected.

Pursuant to Art. 34 HRA, further use may be made of biological material or health-related personal data for research purposes in exceptional cases if: (1) it is impossible or disproportionately difficult to obtain consent or to provide information on the right to dissent, or this would impose an undue burden on the person concerned; (2) no documented refusal is available; and (3) the interests of research outweigh the interests of the person concerned in deciding on the further use of his or her biological material and data (Art. 34 (a) - (c) HRA).

If the material or data are used to carry out a research project that falls under the HRA, authorisation is always required (Art. 45 (1) (a) HRA). If further use takes place on the basis of Art. 34 HRA, authorisation is also always required (Art. 45 (1) (b) HRA).

Authorisation is granted by the competent cantonal ethics committee, which monitors the ethical, legal and scientific requirements of the HRA, and in particular must assess whether the protection of the persons concerned is guaranteed (Art. 51 (1) HRA). The responsible ethics committee is that of the canton in whose territory the research is conducted (Art. 47 (1) HRA). There is no federal ethics committee for human research; federal authorities are also accountable to a cantonal ethics committee.

Data that fall under the HRA and thus refer to a person may not be made accessible as ORD on the basis of the FADP. As for the HRA, the special rules on further use must also be complied with. The term "further use" also includes the storage or recording in biobanks or databases (Art. 24 (c) HRO) and the making available, provision of or transmission of biological material or health-related personal data (Art. 24 (d) HRO). Accordingly, Art. 32-34 HRA must also be complied with for such activities; in connection with this, no authorisation from the ethics committee is required as long as the further use does not take place in the context of a specific research project (e.g. in the case of mere storage in a database).

Non-personal data is not covered by the HRA and can therefore generally be made accessible as ORD. It should be noted that in the case of genetic data (and biological material) there is a prior **information**

⁶⁹ As to this entire subject area, see: MÄTZLER fn. 68 para. 45.

⁷⁰ SHKHFG-RUDIN, fn. 65, Art. 33 N 18.

obligation even where an **anonymisation process** is applied, and anonymisation is only permitted if the person concerned has not exercised his or her right to object.

2.3.3. *Non-human research area*

The HRA does not apply to research with anonymised biological material (Art. 2 (2) (b) HRA) and with anonymously collected or anonymised health-related data (Art. 2 (2) (c) HRA). The data in question are generally unregulated under Swiss law. However, if personal data are processed without the HRA being applicable, the general data protection regulations for the processing of personal data apply.⁷¹ These permit processing for non-personal purposes, in particular for research under certain conditions (Art. 31 (2) (e) FADP for private individuals; Art. 39 FADP for federal authorities), but not the making available of non-anonymised data as ORD.⁷²

Soft law and scientific standards play a central role for both personal data and anonymised data. Many scientific journals and research funding organisations also require proof of ethical justifiability for research projects that do not fall under the HRA. This means that certain requirements must also be followed for such data. These requirements may also extend to the use of ORD. A review is usually carried out by ethics committees of research institutions, such as the ETH Zurich Ethics Committee.⁷³ However, this review is only undertaken if no (legally binding) review by the cantonal ethics committee is required.

From a legal perspective, therefore, only the provisions of the DPA apply. The data may only be made available in anonymised form as ORD. However, it is conceivable that scientific journals and research funding organisations will make further demands.

2.3.4. *Further legislation*

There are further requirements in special laws that can have an impact on ORD. There are special rules, for example, on genetic testing in humans. Art. 10 of the Federal Act on Human Genetic Testing (HGTA)⁷⁴ stipulates, for example, that samples and genetic data must be protected by means of appropriate technical and organisational measures against unauthorised handling and processing. The Transplantation Act, by contrast, authorises the publication of data of general interest relating to the application of the law (Art. 59 (3) Transplantation Act). However, it is stipulated that the persons concerned must not be identifiable. The ordinances provide that certain personal data may be disclosed to

⁷¹ See above, 0.

⁷² See above, 0.

⁷³ See also <<https://ethz.ch/de/die-eth-zuerich/organisation/gremien-gruppen-kommissionen/ethikkommission-on.html>> (last visited on 27 May 2024).

⁷⁴ SR 810.12.

third parties in anonymised form for research purposes, except where the person concerned has consented to disclosure or authorisation has been granted by the competent ethics committee in accordance with Art. 45 HRA (see Art. 34*m* Organ Allocation Ordinance and Art. 49*h* (2) Transplantation Ordinance; also Art. 76 Radiological Protection Ordinance). In the area of medicinal products, however, reports on the results of clinical trials must also be anonymised (Art. 73 (2) Medicinal Products Ordinance). Overall, the use of such data as ORD is scarcely conceivable in view of these strict requirements, especially as reference is regularly made to the (equally strict) requirements of the HRA.

In addition to restrictions, special legal rules can also facilitate the use of certain data, for example by providing for data access. Based on the Cancer Registration Act (CRA), for example, data can be made available for research purposes (Art. 23 (2) CRA). The CRA also refers to the HRA for the collection or further use (Art. 23 (4) CRA). This allows the data to be used for research purposes, but not to be made available as ORD.

However, some decrees also explicitly provide for making data accessible as ORD, for example in the form of *Open Government Data* (OGD). Art. 21 (4) of the Federal Health Insurance Act (German acronym: KVG) stipulates that the competent federal office shall make the data required for performance of the tasks under the KVG available to data providers, research and science, as well as to the public. Similarly, the revision of the Epidemics Act (EpidA) is intended to make usable the data collected and generated under the EpidA.⁷⁵ To this end, data are to be made available to the public and for research purposes in anonymised form (Art. 59 (5) draft revision EpidA).⁷⁶ In line with the federal government's OGD strategy, similar regulations will likely follow in other areas.

2.4. Genetic technology

Genetic engineering law regulates the handling of genetically modified animals, plants and other organisms as well as products derived from such organisms (Art. 3 Gene Technology Act [GTA]). Research, development and production are subject to the Containment Ordinance (ContainO) if they take place in closed systems.⁷⁷ If the research and trials lead to product maturity, different sectoral regulations apply, depending on the type of product. In the case of organisms that are intended to be released

⁷⁵ FEDERAL DEPARTMENT OF HOME AFFAIRS (FDHA), Partial revision of the Epidemics Act, Explanatory report on the opening of the consultation procedure of 29 November 2023, 33.

⁷⁶ EDI, fn. 75, 33. The consultation on the preliminary draft has been completed, see the current status: <https://www.fedlex.admin.ch/de/consultation-procedures/ended/2023#https://fedlex.data.admin.ch/eli/dl/proj/2023/5/cons_1> (last visited on 27 May 2024).

⁷⁷ Ordinance on the Handling of Organisms in Contained Systems, SR 814.912.

into the environment as products, the provisions of the Release Ordinance (German acronym FrSV, e.g. for seeds) apply.⁷⁸ Medicinal products and foodstuffs are subject to product law.⁷⁹

The field of genetic engineering is highly regulated. However, the regulation only covers the handling of genetically modified organisms, i.e. "cellular and non-cellular biological entities" (Art. 5 (1) GTA), not the handling of related data. So far as can be seen, there are no legal restrictions on the publication of genetic engineering data as ORD.

2.5. Environmental law

In addition to the Environmental Protection Act (EPA)⁸⁰ and associated ordinances, environmental law also includes a number of other enactments in the areas of waste, contaminated sites, biodiversity, biotechnology, soil, electrosmog, climate, landscape, noise, air, natural hazards, forests, wood and water.⁸¹

Due to the fact that a large number of people are directly affected, the **principle of publicity** is largely applied in environmental law.⁸² In some cases, the regulations even stipulate that data must be made accessible to the public. According to Art. 10d (1) EPA, the report and results of an environmental impact assessment may be inspected by anyone, unless overriding private or public interests require confidentiality. Manufacturing and business secrecy remains protected in any case, pursuant to Art. 10d (2) EPA. However, this obligation is the responsibility of the publishing authority. Once the environmental impact assessment has been published, the EPA does not impose any restrictions on further availability of the results (e.g. as ORD).

Pursuant to Art. 10e (1) EPA, the authorities are required to inform the public appropriately about environmental protection and the state of environmental pollution. This environmental information comes from the regulatory areas of the EPA or from the area of (federal or cantonal) legislation on nature and cultural heritage protection, landscape protection, water protection, protection against natural hazards, forest conservation, hunting and fishing, genetic engineering and climate protection (Art. 7 (8) EPA).

⁷⁸ Ordinance on the Handling of Organisms in the Environment, SR 814.911.

⁷⁹ Medicinal products: Federal Act on Medicinal Products and Medical Devices (Therapeutic Products Act, TPA), SR 812.21; foodstuffs: Federal Act on Foodstuffs and Utility Articles (Foodstuffs Act, German acronym: LMG), SR 817.0.

⁸⁰ SR 814.01.

⁸¹ <<https://www.bafu.admin.ch/bafu/de/home/themen/recht/geltendes-umweltrecht.html>> (viewed on 27 May 2024).

⁸² THOMAS JUTZI, Unternehmenspublizität, Bern 2017, 48; ROLF H. WEBER, Datenschutz v. Öffentlichkeitsprinzip: Erläuterungen zu den Spannungsfeldern am Beispiel des Zürcher Informations- und Datenschutzgesetzes, Zürich 2010, N 173.

Wherever possible, this environmental information must be made available as open digital datasets (Art. 10e (4) EPA).

Pursuant to Art. 10 of the Geoinformation Act (German acronym: GeoIG),⁸³ **geodata** are also generally accessible to the public and can be used by anyone, provided there are no overriding public or private interests to the contrary. Details are regulated in the Geoinformation Ordinance (German acronym: GeoIV).⁸⁴ This also provides for certain restrictions on the publication of official geodata and assigns three levels of access authorisation (from A to C) to official geodata. The levels of access authorisation for official geodata can be found in Annex 1 GeoIV. Access to level A official geodata is usually granted. In exceptional cases, however, it may be restricted, postponed or refused (Art. 22 (2) GeoIV), for example if reasons of internal security argue against publication. In principle, no access is granted to official geodata of level B access authorisation (Art. 23 (1) GeoIV). There are exceptions to this principle if access does not conflict with confidentiality interests, or if the confidentiality interests can be safeguarded by legal, organisational or technical measures (Art. 23 (2) GeoIV). No access is granted to official geodata of access authorisation level C, without exception (Art. 24 GeoIV). Pursuant to Art. 25 GeoIV, consent can be granted for the use of official geodata for personal or commercial use. However, consent for personal use does not allow authorised persons to make the official geodata accessible as ORD, especially as consent is only granted for personal use by a specific person and only for a fee. However, since access to level A official geodata is granted anyway (Art. 22 (1) GeoIV), it will also be possible to make these accessible as ORD if no exception within the meaning of Art. 22 (2) GeoIV applies.

As a result, it should be noted that research data containing environmental information can generally be published as ORD unless there is an exceptional restriction.

2.6. Chemicals law

The Chemicals Act (ChemA),⁸⁵ the Chemicals Ordinance (ChemO),⁸⁶ the Ordinance on Biocidal Products (OBP)⁸⁷ and the Plant Protection Products Ordinance (PPPO)⁸⁸ do not contain any regulations that prevent the publication of research data from this area as ORD.

⁸³ Federal Act on Geoinformation, SR 510.62.

⁸⁴ Ordinance on Geoinformation, SR 510.620.

⁸⁵ Federal Act on Protection against Dangerous Substances and Preparations, SR 813.1.

⁸⁶ Ordinance on Protection against Dangerous Substances and Preparations, SR 813.11.

⁸⁷ Ordinance on the Placing on the Market and Handling of Biocidal Products, SR 813.12.

⁸⁸ Ordinance on the Placing of Plant Protection Products on the Market, SR 916.161.

However, the Plant Protection Products Ordinance (PPPO) provides for reporting protection for test and study reports (Art. 46 PPPO). This protection does not preclude per se making data available as ORD. However, protected reports may not be used by the authorisation authority for the benefit of another applicant for authorisations for plant protection products, safeners, synergists or additives (Art. 46 (3) PPPO). The reporting protection applies for a period of ten years (Art. 46 (4) PPPO).

The Federal Office of Public Health (FOPH) may also make data from the radon database available to third parties for research purposes. However, this is linked, among other things, to the condition that the data is not passed on (Art. 162 (5) (b) Radiation Protection Ordinance). Data of this type may therefore not be made accessible as ORD.

2.7. Food law

The legal basis for data from the food sector is primarily the Foodstuffs Act (German acronym: LMG)⁸⁹ and the Ordinance on the Enforcement of Foodstuffs Legislation (German acronym: LMVV).⁹⁰ Art. 40 (1) LMG stipulates that the Confederation shall research and procure the scientific basis required for the application of the LMG. It may carry out these surveys itself or in co-operation with the cantons (Art. 40 (2) LMG). If this is the case, the results of research work and surveys may not be made accessible to the public if they allow conclusions to be drawn about the manufacturers, distributors or products concerned (Art. 24 (4) (b) LMG). It is conceivable that the institutions within the ETH Domain conduct research based on Art. 40 of the LMG, which could prevent the publication of research data from the food sector as ORD. Beyond this, there are no (further) restrictions in this area of the law that prevent research data from being made accessible as ORD.

2.8. Energy and nuclear energy law

In energy law, there are restrictions on the publication of research data for the protection of critical infrastructures. Critical infrastructures are processes, systems and facilities that are essential for the functioning of the economy and the well-being of the population. For Switzerland, the spectrum of critical infrastructures in energy law includes the areas of natural gas supply, oil supply, electricity supply, water supply, district heat and heat for processes, waste and wastewater.⁹¹ The inventory of critical infrastructures (CIP inventory) defines buildings and facilities that are of strategic importance from either a national or cantonal perspective. The inventory is classified in its entirety as secret. Extracts

⁸⁹ Federal Act on Foodstuffs and Utility Articles, SR 817.0.

⁹⁰ SR 817.042.

⁹¹ FEDERAL OFFICE FOR CIVIL PROTECTION, National Strategy for Critical Infrastructure Protection (CIP), Comprehensive Approach to Ensuring the Availability of Essential Goods and Services of 16 June 2023, Official Federal Gazette 2023 1659, 7-8.

containing only part of the information (e.g. from a canton or a sector) are generally classified as confidential.⁹² If research data concerns information on critical infrastructures, they may not be made publicly accessible as ORD.

In the field of **nuclear energy**, there is a public interest in secrecy with regard to various matters, e.g. relating to the utilisation of radioactive elements and the operation of nuclear power plants, in order to ensure safety and protection against acts of sabotage or terrorist attacks. Art. 91 (1) (b) of the Nuclear Energy Act (NEA)⁹³ makes breaches of secrecy a criminal offence. Accordingly, anyone who discloses or makes available to unauthorised parties secret facts or measures that serve to protect nuclear installations, nuclear materials or radioactive waste from the effects of third parties, or from the effects of war, is liable to prosecution.

It is not possible to state in abstract terms which information is covered by the criminal provision on the violation of secrecy in Art. 91 (1) (b) NEA. When using research data in connection with nuclear energy, it must therefore be ensured that these are only made accessible as ORD if they can be made accessible to the public in accordance with Art. 74 (1) NEA, and do not pertain to secret facts and measures that serve to protect nuclear facilities, nuclear materials or radioactive waste from the effects of third parties or from the effects of war. Anyone who makes such research data accessible as ORD is liable to prosecution under Art. 91 (1) (b) NEA.

A further hurdle for ORD in connection with data from nuclear energy can be found in Art. 13 of the Nuclear Energy Ordinance (NEO).⁹⁴ Art. 13 NEO provides for an authorisation requirement for the export and transfer of technology relating to nuclear materials. Technology in this context means specific knowledge in the form of technical data or technical support required for the development, production or use of nuclear materials that is not generally accessible or does not serve basic scientific research. Authorisation is therefore required if research data containing such information are to be made accessible as ORD. Authorisation for export and transfer is granted if the authorisation requirements pursuant to Art. 7 (a) (f) NEO are met. In particular, the protection of people and the environment, as well as nuclear safety and security, must be guaranteed, and there must be no obstacles present stemming from policies of non-proliferation of nuclear weapons supported by Switzerland. Whether technologies relating to nuclear materials comply with export and transfer authorisations must be examined on a case-by-case basis. These research data cannot be made accessible as ORD without such authorisation for export and transfer.

⁹² <<https://www.babs.admin.ch/de/die-kritischen-infrastrukturen>> (viewed on 27 May 2024).

⁹³ SR 732.1.

⁹⁴ SR 732.11.

In energy and nuclear energy law, there are legal restrictions that prevent the publication of certain research data as ORD. In energy law, the restrictions relate to data on the inventory of critical infrastructure, which must be treated as secret or confidential. In the field of nuclear energy, there are restrictions on information that serves to protect nuclear facilities, nuclear materials and radioactive waste from the effects of third parties or from the effects of war, and on data whose export or transfer would jeopardise nuclear safety.

2.9. Animal welfare law

In animal protection law, the Animal Welfare Act (AniWA)⁹⁵ and the Animal Protection Ordinance (AniPO),⁹⁶ which regulate the protection of vertebrates (i.e. mammals, fish, birds, amphibians and reptiles), must be complied with first and foremost. Invertebrates (e.g. snails, spiders, worms), are excluded from the scope of application. In addition to animal protection and animal welfare law, a number of other areas of law affect animals, e.g. animal breeding, veterinary law, direct agricultural payments, species protection, hunting and fishing law, and food law.

The analysis of the relevant legal bases in animal welfare law shows that there are no legal restrictions on the publication of research data as ORD.

2.10. Financial markets law

In the area of financial markets law, particular attention must be paid to compliance with banking secrecy. The duty of confidentiality pursuant to Art. 47 of the Banking Act (German acronym: BankG)⁹⁷ applies to all knowledge arising from the bank's business relationship with the client, in particular from banking contracts, as well as enquiries and offers for other banking transactions and business transactions between banks.⁹⁸

The duty of confidentiality applies to all persons working in a bank or for it on a contractual basis. A bank may only grant academic staff access to customer data if an employment or contractual relationship exists with them (Art. 47 (1) BankG). In any case, the anonymisation of customer data in any publication remains mandatory unless customers expressly consent to disclosure.⁹⁹ Anonymised bank

⁹⁵ SR 45.

⁹⁶ SR 455.1.

⁹⁷ Federal Law on Banks and Savings Banks, SR 952. 0.

⁹⁸ BEAT KLEINER/RENATE SCHWOB/CHRISTOPH WINZELER, Kommentar zum Bundesgesetz über die Banken und Sparkassen vom 8. November 1934 sowie zu der Verordnung vom 17. Mai 1972 (V) und der Vollziehungsverordnung (VV) vom 30. August 1961 (VV) – mit Hinweisen auf das Bankenrecht der Europäischen Union, auf das Allgemeine Dienstleistungsabkommen (GATS) und mit Erläuterungen zu den Massnahmen gegen die Geldwäscherei, Zobl/Schwob/Winzeler/Kaufmann/Weber/Kramer (eds.), Zürich 2015, Art. 47 N 8-9.

⁹⁹ BankG-Komm., KLEINER/SCHWOB/WINZELER, fn. 98, Art. 47 N 335, 360.

data are no longer personal data if, in the ordinary course of events, no data subject can avail him- or herself of the means that can reasonably be used for re-identification. Bank data are removed from the protection of banking secrecy if they are anonymised.¹⁰⁰ If bank data have been transmitted to researchers in anonymised form, it can generally be assumed that the publication of these data as ORD does not violate banking secrecy and is therefore permissible. Data that are subject to banking secrecy can thus only be made accessible in anonymised form as ORD.

As a result, it is clear that research data subject to banking secrecy may not be made accessible as ORD. If the bank customer data are anonymised, they can be published as ORD.

The regulations governing financial services¹⁰¹ and financial institutions¹⁰² do not impose any legal restrictions on ORD.

3. Third party rights

Making research data accessible may conflict not only with legal requirements, but also with the rights of third parties. The focus here is on copyright, claims arising from the protection of secrets under criminal law (Art. 162 SCC), claims arising from the UCA (Art. 5 (c) and Art. 6 UCA) and claims arising from data protection law. Patents, on the other hand, cannot be used to prevent research data from being made accessible.

3.1. Copyright

We assume that, as a rule, neither works of literature and art, nor protected performances, nor computer programs will be made available in whole or in part as ORD. Before ORD is made available, however, **confirmation of whether the data or parts thereof contain copyrighted works** must always be performed.¹⁰³ This is the case, for example, if sufficiently long sequences of source code or of texts, images or photographs are made accessible. If this is the case, the copyright holders of these works must be asked whether they grant access to their works.

Large quantities of research data that are made accessible as ORD will regularly qualify as databases within the meaning of copyright law. If **structured databases** are involved, these may be protected by copyright. Before making data available as ORD, confirmation of whether the data qualify as a database

¹⁰⁰ CÉLIAN HIRSCH/ÉMILIE JACOT-GUILLARMOD, Les données bancaires pseudonymisées - Du secret bancaire à la protection des données, SZW 2020, 151 et seq., 156.

¹⁰¹ Federal Act on Financial Services (Financial Services Act, FinSA), SR 950.1.

¹⁰² Federal Act on Financial Institutions (Financial Institutions Act, FinIA), SR 954.1.

¹⁰³ See above, B.1.2.

that could be protected by copyright must always be performed. If this is the case, the rightsholders must be asked whether they grant access to the database.

The copyrights belong to the persons who created the database (Art. 6 CopA). With regard to databases created by employees of an institution within the ETH Domain, the copyrights to the databases belong to those employees (Art. 36 (1) ETH Act). Although this provision does not appear to make much sense, especially since the copyrights to source code are transferred by law to the institutions within the ETH Domain (Art. 36 (2) ETH Act), it is unambiguous from the provision in Art. 36 (1) and (2) ETH Act. Employees can thus decide for themselves whether they wish to make databases accessible as ORD, provided that the respective institution within the ETH Domain has not issued an internal regulation that prescribes the transfer of copyrights to databases to the institution or the making available of research data (and/or databases) as ORD. If a **database has been created by a third party, the consent of the third party must be obtained**. Confirmation of whether the authors of the database have assigned their rights to other third parties (e.g. to a university, a publisher or a commercial provider) must always be performed. Where this is the case, their consent must be obtained.

3.2. Patents

Patents are granted for **inventions**, i.e. for **technical teachings**.¹⁰⁴ They give their proprietor the right to prohibit others from using the invention commercially (Art. 8 (1) PatA). Use is deemed to include, in particular, manufacturing, storage, offering, placing on the market, importing, exporting, carrying in transit and possession for any of these purposes (Art. 8 (2) PatA). A distinction must be made between **product and process patents**. In the case of product patents, the manufacture and commercialisation of the patented invention are deemed to constitute use. This covers all (but only) acts relating to the patented product; in addition to manufacturing, this also includes storing, offering, placing on the market (etc.) of such a product. In the case of process patents, use is deemed present if the process is applied, i.e. if the process steps provided for in the patent claims are carried out.

Research data made available as ORD may contain patented inventions. Although rare, this cannot be ruled out. However, making an invention available via the internet **does not constitute the use of an invention** within the meaning of patent law, because it constitutes neither the manufacture of a product nor the carrying out of a process. Therefore, the patent proprietor cannot prohibit others from making the invention available.

¹⁰⁴ MARK SCHWEIZER/HERBERT ZECH, in: Schweizer/Zech (eds.), Stämpfli Handkommentar, Patentgesetz (PatG), Bundesgesetz über die Erfindungspatente vom 25. Juni 1954, Bern 2019, Art. 1 N 10; BGer 4A.12/1995 of 31 July 1996, E. 4, in: sic! 1997, 77 et seq. In its decision, the Federal Supreme Court defined a technical invention as a "teaching for planned action using controllable natural forces to directly achieve a causally foreseeable outcome".

It should also be noted that patents are only granted if the **invention is disclosed in the patent application**. This means that the invention must be set out in the patent application so clearly and completely that it can be carried out by a person skilled in the art on the basis of the patent specification and taking into account the general specialised knowledge in the relevant field (Art. 50 (1) PatA).¹⁰⁵ Since the patent specification is published on the Patent Office's website when the patent is granted, the invention is already publicly accessible. If research data made available as ORD contain a patented invention, this does not disclose any information that is not already publicly available.

3.3. Claims arising from the protection of secrets under criminal law

If research data is made accessible as ORD, despite researchers and/or the institution within the ETH Domain being legally or contractually obliged to preserve confidentiality, this constitutes an offence against Art. 162 SCC. The natural person who has made the data accessible may be punished with a custodial sentence of up to three years or a fine upon complaint by the person with the rights to claim confidentiality (Art. 162 SCC).

The **person with rights to claim confidentiality** is authorised to file a criminal complaint. As a rule, the rightsholder will be another research institution or a company that has made research data accessible to a researcher or an institution within the ETH Domain and has obliged the researcher or the institution to preserve confidentiality. The rightsholder can not only apply for a penalty, but also demand injunctive relief and compensation in damages. The claim for damages is based on general tort law (Art. 41 (CO) in conjunction with Art. 162 SCC). Although the claim for injunctive relief is not expressly provided for, it can be inferred from general tort law (Art. 41 et seq. CO). This is because general Swiss tort law not only provides a claim for damages, but also a claim for injunctive relief, as is fair.¹⁰⁶

3.4. Claims arising from UCA

The UCA applies to all actions that are designed to influence competition in a (specific) market. This includes all actions that are **market-relevant, market-orientated or competition-oriented** and that can affect the relationship between competitors, or between suppliers and customers. However, as long as these activities are carried out in an academic context, the UCA does not apply to scientific research

¹⁰⁵ HGer SG, sic! 2009, 875 et seq., 879 et seq. - "Dichtmasse"; SHK PatG-Sutter/Hochreutener, fn. 104, Art. 50 N 3 et seq.

¹⁰⁶ MARTIN A. KESSLER, in: Widmer Lüchinger/Oser (eds.), Basler Kommentar, Obligationenrecht I, Art. 1-529 OR, Basel 2020, Art. 43 N 4; along these lines also MARTIN ECKERT, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 2016, 245 et seq., 272 and URS HESS-ODONI, Die Herrschaftsrechte an Daten, in: Jusletter of 17 May 2004, para. 39.

or the publication of its results.¹⁰⁷ The UCA does apply to collaborations with private companies and when the research results (e.g. from a start-up) are to be utilised on the market.

The taking over and making available of research data as ORD may violate the **prohibition on direct taking over** (Art. 5 (c) UCA) or be qualified as a **breach of manufacturing and trade secrets** (Art. 6 UCA). The latter is only the case, however, if an infringer has gained access to the data through espionage or otherwise obtained it unlawfully.¹⁰⁸

Any persons who are threatened with or sustain damage to their customer base, their credit or professional reputation, their business operations or otherwise to their economic interests as a result of a violation of the UCA may request the court to enjoin the infringement, redress the effects of the infringement, and award damages and disgorgement of profits. (Art. 9 UCA). A violation of Art. 5 (c) or Art. 6 UCA is also punishable as a criminal offence; the offender is liable to up to three years in prison or a fine (Art. 23 UCA). The *data owner*, i.e. the **holder of de facto control over the data** which is legally protected by Art. 5 (c) and Art. 6 UCA, is entitled to bring an action for injunctive relief, redress and damages, or disgorgement of profits, and to file a criminal complaint.

3.5. Data protection claims

Data protection law **does not** give data subjects a **comprehensive right of control** over data pertaining to them, but it does give them certain rights with which they can control and restrict the use of the data to a certain extent. These possibilities are significantly broader if the data is processed by a private person or entity, in particular a company. In certain cases, processing by companies is based on the consent of the data subject, which can be withdrawn at any time.¹⁰⁹ In addition, data subjects may object to the processing of data concerning them (Art. 30 (2) (b) FADP). The consequence of both is that the data may only be processed by the private individual if the private individual has an overriding interest in the processing (Art. 31 FADP).

The processing of personal data by federal bodies always has a **legal basis**. Consent by the data subjects is not required for this processing. This also applies to the processing of personal data for research purposes by the institutions within the ETH Domain. The fact that the data subjects regularly give their consent to the processing of personal data for research purposes does not change this legal situation. **Obtaining consent** is undoubtedly to be welcomed from an ethical (research) perspective, is provided for by numerous standards and is established practice in many areas, but is **not required under data protection law**, neither for processing as part of a research project nor for making the

¹⁰⁷ Federal Supreme Court 6B_188/2013 of 4 July 2013, E. 6.3, with further references.

¹⁰⁸ See above, B.1.5.

¹⁰⁹ BSKDSG-BÜHLMANN/REINLE, fn. 59, Art. 6 N 316; SHKDSG-BAERISWYL, fn. 59, Art. 6 N 84.

research data available as ORD in anonymised form. Since the processing of personal data for research at the institutions within the ETH Domain is not legally based on consent, the data subjects cannot legally prevent the processing of data concerning them by withdrawing their consent or by exercising a right of objection or erasure. Data subjects therefore have no rights to prevent their "personal data" from being made accessible as ORD.

Personal data may **only** be made **accessible in anonymised form as ORD** due to general data protection legislation.¹¹⁰ If this requirement is met, the FADP does not apply to making the data accessible. For this reason alone, data subjects have no data protection claims that they could assert to prevent research data being made available as ORD.

4. Contractual restrictions

Research projects are often carried out as part of a collaboration among several universities and/or in cooperation with companies. Such collaborations are usually governed by contracts which contain provisions governing the confidentiality of research results. These **confidentiality obligations** may result in restrictions with regard to ORD. Such obligations may be provided for in cooperation or licence agreements, in non-disclosure agreements (NDA) or in material transfer agreements (MTA). However, restrictions on ORD can also arise from **other contractual agreements** governing the handling of research data.

Such contractual requirements may **conflict with the ORD strategy** of an institution within the ETH Domain or its concrete implementation in laws or internal guidelines. In such cases, the question arises as to whether the contractual agreement is valid. The freedom of contract principle applies in respect of the drafting and structuring of contracts. However, restrictions may arise from Art. 19 (2) CO, pursuant to which a contractual agreement may not violate mandatory public policy, morality or public order. Contracts with impossible, unlawful or immoral content are also void (Art. 20 (2) CO). Contracts that excessively bind one party are also inadmissible (Art. 27 (2) Swiss Civil Code [CC]). Depending on how they are structured, ORD requirements may qualify as mandatory law. A contract is **unlawful** within the meaning of Art. 19/20 CO if its content contradicts a mandatory objective, private or public law norm of Swiss (federal or cantonal) law, whether written or unwritten.¹¹¹ Whether a legal norm is mandatory or not is determined by the interpretation of the relevant norm.¹¹²

¹¹⁰ See above, 0.

¹¹¹ BSK ORI-MEISE/HUGUENIN, fn. 106, Art. 19/20 N 15; AHMET KUT/CHRISTOPH BAUER, in: Atamer/Furrer (eds.), Handkommentar zum Schweizer Privatrecht, Obligationenrecht - Allgemeine Bestimmungen - Art. 1-183 OR, Zurich 2023, Art. 20 N 13; BGer 4A_173/2010 of 22 June 2010, E. 2.2.

¹¹² BSK OR I-MEISE/HUGUENIN fn. 106, Art. 19/20 N 20 f; CHK OR-KUT/BAUER fn. 111, Art. 20 N 14; BGE 143 III 600, E. 2.8.1.



If a contract between researchers and a counterparty contains an agreement that is not in line with the university's ORD strategy, a two-stage review must be carried out. The first step is to check whether the legal norm which the contract potentially violates is a **statutory provision** within the meaning of Art. 19/20 CO. This is the case, for example, with the ETH Act, though that act contains no requirements regarding ORD. Internal guidelines must be examined to determine they qualify as statutory provisions within the meaning of Art. 19/20 CO. The second step is to analyse whether the **provision** in question is **mandatory**. If this is the case, the contract is null and void (Art. 20 (1) CO). However, according to prevailing legal scholarship and practice, the consequence of nullity does not arise automatically, but only "if this legal consequence is expressly provided for by law or follows from the meaning and purpose of the infringed legal norm".¹¹³ According to the principle of partial nullity, nullity only extends to the extent required by the protective purpose of the infringed legal norm.

The protective purpose of provisions relating to ORD should not generally require complete nullity of the contract. Rather, it should comport with the purpose of the relevant provision that only those provisions of the contract that violate the ORD-relevant provision would be considered null and void. Exceptions only apply if it can be assumed that the entire contract would not have been concluded without the unlawful content.¹¹⁴ This may be the case, for example, if a cooperation agreement provides for an obligation to keep research data confidential that is null and void due to a breach of an ORD provision, and the contracting party would not have concluded the agreement if it had been aware that the research data had to be made accessible as ORD.

Licence agreements may also give rise to restrictions in respect of ORD. In addition to confidentiality obligations, licence agreements may, for example, contain certain geographical or temporal restrictions on use that conflict with ORD. Requirements for the transfer and publication of data (e.g. the obligation to publish data on a specific platform) may also conflict with ORD requirements of the institutions within the ETH Domain.

5. Liability

If researchers disregard the restrictions relating to ORD and cause damage to third parties, the general rules on liability apply.

¹¹³ BSK OR I-MEISE/HUGUENIN fn. 106, Art. 19/20 N 54 with further references; BGE 143 III 600, E. 2.8.1; BGE 134 III 438, E. 2.2; BGE 123 III 292, E. 2.e.aa.

¹¹⁴ BSK OR I-MEISE/HUGUENIN fn. 106, Art. 19/20 N 64a; CHK OR-KUT/BAUER fn. 111, Art. 20 N 49; BGer 4C.156/2006 of 17 August 2006, E. 3.4; BGE 143 III 558, E. 4.1.1; BGE 124 III 57, E. 3.c with further references

In **external relations** (i.e. vis-à-vis third parties), the institutions within the ETH Domain are liable, irrespective of the fault of their employees, for damage unlawfully caused to third parties by their employees in the performance of their official duties (Art. 3 (1) in conjunction with Art. 19 (1)(a) Liability Act [German acronym: VG] in conjunction with Art. 5 (1) ETH Act). Special provisions apply to certain areas of law (e.g. Art. 30 et seq. GTA), which take precedence over the VG (Art. 3 (2) VG), but these are unlikely to be relevant here. Contracts also sometimes contain provisions governing the consequences of breaches of contract, e.g. by stipulating contractual penalties.

In **internal relations** (i.e. in the relationship between the employees and the ETH Domain institution), the respective internal guidelines apply, namely the rules on making research data accessible as ORD, in addition to rules on scientific integrity and guidelines on how to proceed in the event of scientific misconduct.

D. LEGAL IMPLEMENTATION OF ORD

1. Preliminary remarks

The constitution contains the basic state norms. An important part of the constitution are fundamental rights, guaranteeing individuals essential rights vis-à-vis the state. Not only is the state itself considered the “state”, but also whoever acts on behalf of the state (Art. 35 (2) Federal Constitution of the Swiss Confederation [German acronym: BV]). The **institutions within the ETH Domain** fulfil state tasks and are **bound to honour fundamental rights** in their actions. These requirements must also be observed when implementing ORD.

Provided there are no legal restrictions and third parties have no rights to the research data, or where they waive the exercise of these rights, research data can be made freely accessible as ORD. From a legal perspective, **ORD** can be **accessed completely freely**, i.e. without concluding a licence agreement and without agreeing to terms of use, and therefore without imposing restrictions on users when accessing and using the data.

As a rule, however, the operator of an ORD platform will only make the research data available on the basis of a **licence agreement** in order to ensure compliance with certain conditions (e.g. indication of the source or compliance with scientific standards). The ETH Board's position paper also stipulates that ORD should be used on the basis of a licence.¹¹⁵

¹¹⁵ ETH BOARD, Open Research Data, Position of the ETH Domain, 5.

2. Constitutional framework

An ORD strategy can be implemented in various ways. In order to implement the approach effectively, it may be necessary to oblige researchers to make their research data publicly accessible. Such an obligation may be relevant from a fundamental rights perspective. The fundamental rights of academic freedom, the guarantee of property and economic freedom may be affected.

2.1. Fundamental rights relevant to ORD

The most important fundamental right in connection with ORD is **academic freedom**, which protects academic scholarship and research (Art. 20 BV).¹¹⁶ Researchers who are required to handle research data in a certain way due to ORD requirements are affected. This is in contrast to the academic freedom of other researchers and members of the scientific community. Such persons may be dependent on access to third-party research data for their own research. It is questionable whether research data falls under the **guarantee of ownership** (Art. 26 BV). The guarantee of ownership protects all pecuniary rights of private property, including intellectual property rights as well as rights *in rem*.¹¹⁷ Whether data are also covered by the constitutional concept of ownership has not yet been resolved, but scholars tend towards the negative.¹¹⁸ The **economic freedom** (Art. 27 BV) of potential co-operation partners may also be affected. This protects free private economic activity, in particular the free choice of profession, free access to and the free pursuit of gainful employment (Art. 27 (2) BV).¹¹⁹ The focus here is on the elements of “free exercise of entrepreneurial activity” and “freedom of contract”. An obligation to publish research data deprives cooperation partners of the opportunity to decide for themselves on the use of the research data, e.g. through profitable licensing or sale.

2.2. Restriction on fundamental rights

Fundamental rights are not absolute, but can be restricted in accordance with Art. 36 of the Federal Constitution. The prerequisite is that a legal basis exists, the restriction is in the public interest and is proportionate (Art. 36 BV). These requirements must be taken into account when designing an ORD strategy.

¹¹⁶ MAYA HERTIG, in: Waldmann/Besler/Epiney (eds.), Basler Kommentar, Schweizerische Bundesverfassung (BV), Basel 2015, Art. 20 N 5.

¹¹⁷ BSKBV-VALLENDER/HETTICH, fn. 116, Art. 26 N 19; GIOVANNI BIAGGINI, in: Biaggini (ed.), Fed.Const.-Kommentar, Bundesverfassung der Schweizerischen Eidgenossenschaft, Zurich 2017, Art. 26 N 12.

¹¹⁸ THOUVENIN, SJZ 2017, 21 et seq., 21; BV KommBIAGGINI fn. 117, Art. 26 N 12.

¹¹⁹ BV Comm, BIAGGINI fn. 117, Art. 27 N 4; BSK BV.-Uhlmann, fn. 116, Art. 27 N 4 with reference to BGE 131 I 333, E. 4 and BGE 137 I 167, E. 3.1.

The requirement of a sufficient **legal basis** must be taken into account; the obligation to make research data accessible as ORD should ideally be anchored in a statute in the formal sense. Whether anchoring an ORD requirement in internal guidelines is sufficient would have to be examined on a case-by-case basis, and also depends on the scope of the obligation. The **public interest** must be weighed against the interest of other researchers and the general public in the research data.

Three aspects need to be examined in terms of **proportionality**: suitability, necessity and proportionality in the narrow sense of the term (reasonableness). Measures that interfere with fundamental rights must be suitable for achieving an objective that is in the public interest.¹²⁰ The interference with a fundamental right must also be necessary, i.e. it may only go as far as is necessary to achieve the objectives in the public interest. In addition, the public interests must outweigh the conflicting fundamental rights of the data subjects, i.e. a balancing of interests must be carried out. Safeguarding proportionality is likely to be the decisive factor when introducing an ORD strategy. With regard to the **suitability** of a strategy for safeguarding the public interest, aspects such as accessibility and the conditions under which access to the data is granted must be taken into account. The lower the barriers to access the data for other researchers, the more likely it is that the public interest will be met. As to the criterion of **necessity**, it will be necessary to estimate how far the obligation must go in order to achieve the public interest pursued by the provision. The least invasive measure must be chosen in each case, which means that the fundamental rights of the researchers and cooperation partners in question must be protected as far as possible. In addition to freedom of research, this also includes the guarantee of ownership and of economic freedom, which are affected by a provision that restricts the free availability of any existing intellectual property rights to research data, and the protection of research data as trade secrets.¹²¹ These points are likely to be important when assessing proportionality in the narrow sense.

3. Licence agreements

3.1. Subject matter

In a **licence agreement**, the licensor authorises the licensee to use an intangible asset to the agreed extent.¹²² A fee (licence fee or royalty) is not part of the objectively essential content of the contract, but

¹²⁰ BV Comm, BIAGGINI fn. 117, Art. 5 N 21 with reference to BGE 136 I 29, E. 4.2; BSK BV-EPINEY fn. 116, Art. 5 N 70.

¹²¹ See above, B.1.5.

¹²² Reto HILTY, Lizenzvertragsrecht, Bern 2002, 5 et seq.; BSK ORI-AMSTUTZ/MORIN, fn. 106, Einl. vor OR 184 et seq. N 238; ROLAND VON BÜREN, in: David/von Büren (eds.), Schweizerisches Immaterialgüter- und Wettbewerbsrecht (SIWR), I/1, Grundlagen, Basel 2002, 295.

is ordinarily included.¹²³ A licence agreement can be **used** to permit the **use of all types of intangible assets**.

A genuine licence agreement is present if the intangible asset whose use is being licensed is protected by an intellectual property right (e.g. a patent or copyright). A non-genuine licence agreement governs the use of an intangible asset that is not (or is no longer) protected by an intellectual property right,¹²⁴ in particular the use of know-how. This includes, in particular, information that is protected as manufacturing and trade secrets against unauthorised use by third parties under Art. 6 UCA and Art. 162 SCC. If the licence permits the use of (supplementary) know-how, in addition to permitting the use of intellectual property protected by *erga omnes* rights, this constitutes a mixed licence agreement.¹²⁵ **Licence agreements for data** are generally qualified as **non-genuine licence agreements**. If the data represent copyright-protected works or services, a mixed licence agreement exists.

3.2. Formal requirements

The conclusion of a contract is only subject to requirements as to form if provided for by law or agreed by the parties (Art. 11 (1) and Art. 16 (1) CO). Inasmuch as a licence agreement is a contract that is not governed by specific law (a so-called innominate contract), the law **does not stipulate any formal requirements**. Unless the parties have agreed otherwise, a licence agreement can therefore be concluded in purely electronic form, orally or by implication.¹²⁶

3.3. Content

Contract law is based on the principle of freedom of contract. This includes the freedom to draft/structure the content of contracts, so-called **freedom of content**.¹²⁷ Within the general limits of contractual freedom (in particular Art. 19/20 CO and Art. 27 CC)¹²⁸, the parties may **freely structure licence agreements**. This also applies to ORD. The institutions within the ETH Domain are thus free to define the terms of the licence agreements under which research data are to be made accessible as ORD.

¹²³ BSK ORI-AMSTUTZ/MORIN, fn. 106, Einl. vor OR 184 et seq. N 238; EUGEN MARBACH/PATRIK DUCREY/GREGOR WILD, Immaterialgüter- und Wettbewerbsrecht, Bern 2017, para. 925; MAGDA STREULI-YOUSSEF, in: Streuli-Youssef (ed.), Swiss Intellectual Property and Competition Law (SWIT), V/1, Basel 2020, 22.

¹²⁴ ROBERT M. STUTZ/STEPHAN BEUTLER/MARC HOTTINGER, in: Stutz/Bleuler/Hottinger (eds.), Stämpflis Handkommentar, Designgesetz (DesG), Bern 2022, Art. 15 N 12; CLAIRE HUGUENIN, Obligationenrecht, Allgemeiner und Besonderer Teil, Zurich 2019, para. 3792; HILTY, fn. 122, 15.

¹²⁵ ROLAND FISCHER/LARA DORIGO, in: Weinmann/Münch/Herren (eds.), Schweizer IP-Handbuch, Intellectual Property - Konzepte, Checklisten und Musterdokumente für die Praxis, Basel 2021, § 17 para. 0.8.

¹²⁶ HILTY, fn. 122, 275; VON BÜREN, fn. 122, 332; SHK DesG-Stutz/Beutler/Hottinger, FN.124, Art. 15 N 21.

¹²⁷ BSK OR I-MEISE/HUGUENIN fn. 111, Art. 19/20 N 5 et seq. with reference to BGE 115 II 237, E. 4.d; PETER GAUCH/WALTER R. SCHLUEP/JÖRG SCHMID/SUSAN EMMENEGGER, Swiss Code of Obligations General Section, Zurich 2020, margin no. 626.

¹²⁸ See above, C.4.

In particular, it is possible to grant the licence free of charge (so-called gratuitous or free licence) or in exchange for payment of a **licence fee**. The parties are free to determine the licence fee. In practice, there are numerous variations on contract terms for determining and calculating licence fees, such as one-off licence fees, milestone lump-sum payments on reaching certain targets, periodic fees, sales or profit-based fees, and unit licences.¹²⁹ The parties often combine a lump sum to be paid upon conclusion of the contract (so-called downpayment) with a turnover-based licence fee to be paid periodically (e.g. annually or quarterly).¹³⁰

The parties can also freely determine the scope of the **rights of use** granted by the licence. In particular, use can be restricted in temporal (e.g. one year) or geographical scope (e.g. a specific country), or for specific purposes (e.g. purely scientific, excluding commercial use).

In addition, it can (and should) be stipulated whether the licensee is entitled to grant a **sub-licence** to third parties which entitles them to use the intangible asset. The sub-licence cannot grant more extensive (but can grant less extensive) powers than the main licence. Since there is some dispute on the question of whether the licensee is entitled to grant a sub-licence if the licence agreement does not contain a provision to this effect,¹³¹ the contract should also (and in particular) contain specific provisions setting out when the licensee is not to have the right to grant a sublicense.

4. Competition law aspects

Certain competition legislation must be observed when implementing ORD. The Cartel Act (CartA) applies to companies under private and public law that participate in competition. As a basic principle, private individuals are not subject to the Cartel Act.¹³² Competition law thus does not apply to researchers who make their data public. The operators of ORD platforms, on the other hand, are likely to be subject to competition law.

Depending on the conditions of access, problems could arise from the perspective of the operators of ORD platforms if an operator were to qualify as a relatively powerful or dominant company. According to Art. 4 (2) CartA, a company is deemed to be **dominant** if it is able to behave independently to a

¹²⁹ In respect of the different variants, see: FISCHER/DORIGO, fn. 125, § 17 para. 6.1; VON BÜREN, fn. 122, 347 et seq.; HILTY, fn. 122, 486.

¹³⁰ For more detail on the so-called downpayment FISCHER/DORIGO, fn. 125, § 17 para. 6.3, 6.4.

¹³¹ HILTY, Fn. 122, 758 et seq.; VON BÜREN, Fn. 122, p. 314 et seq.; SHK DesG-STUTZ/BEUTLER/HOTTINGER, Fn. 124, Art. 15 N 15.

¹³² BERNHARD RUBIN/MATTHIAS COURVOISIER, in: Baker & McKenzie (ed.), Stämpfli Handkommentar, Kartellgesetz (KG), Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen, Bern 2007, Art. 2 N 9; RETO HEIZMANN/MICHAEL MAYER, in: Zäch et al. (Eds.), CartelA-Kommentar, Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen, Zürich 2018, Art. 2 N 25.

significant extent on a market. A key factor in assessing whether market dominance exists is market share; subject to special circumstances,¹³³ this would have to be above 50% for market dominance to be assumed.¹³⁴ As research data are collected and processed all over the world, it can hardly be assumed that an ORD platform will be categorised as dominant in the market. The existence of relative market power is more obvious. According to Art. 4 (2)^{bis} CartA, a company is deemed to **have relative market power** if other companies are dependent on it in such a way that there are no adequate and reasonable alternatives. In this respect, too, the research data in question must be analysed to determine whether they can be substituted. Research data that are, for example, part of the state of the art or research and therefore found in other sources can be substituted. In the case of research data which cannot be substituted, there are no alternative options for other researchers, which is why there is likely to be relative market power if this research data are offered as ORD by a research institution.

Holding a relatively powerful or dominant market position is not in itself unlawful; only certain **abusive behaviour** is unlawful (Art. 7 (1-2) CartA). Art. 7 (2) (a) CartA may be relevant. **If** the owner of an essential facility or information **refuses access to third parties** without there being legitimate business reasons for doing so, this may constitute an unauthorised refusal to deal. An essential facility always exists if access to it is objectively necessary in order to operate on a downstream market.¹³⁵ Whether an ORD platform is considered an essential facility must be examined on a case-by-case basis. A violation of Art. 7 (2) (a) CartA would only exist if access to certain research data were restricted for certain groups of people without objective reasons being given.

Abusive behaviour could also consist of **setting unfair prices or unfair terms and conditions** (Art. 7 (2) (c) CartA), e.g. if a (high) price is charged for access to the data or if access to the ORD platform is subject to particularly strict conditions that differ significantly from the conditions of other ORD platforms. Whether these elements are made out would have to be resolved on a case-by-case basis. With regard to the amount of the licence fee, it should be noted that restricting access for economic reasons by charging a licence fee is permissible from a cartel law perspective, provided the fee is intended to compensate for a financial expense in connection with the provision of the data. This can include costs from the merging of data records, anonymisation or facilitating interoperability.¹³⁶

¹³³ Such special circumstances may exist, for example, where certain data can only be collected exclusively from a research institution and that institution has an obligation to provide the data exclusively on its platform.

¹³⁴ JÜRIG BORER, in: Orell Füssli Kommentar, Wettbewerbsrecht I, Schweizerisches Kartellgesetz (KG) mit den Ausführungserlassen sowie einschlägigen Bekanntmachungen und Meldeformularen der WEKO, Zurich 2011, Art. 4 N 19; SHK KG-Roland KÖCHLI/PHILIPPE M. REICH, fn. 132, Art. 4 N 38.

¹³⁵ MARC AMSTUTZ/BLAISE CARRON, in: Amstutz/Reinert (eds.), Basler Kommentar, Kartellgesetz (KG), Basel 2021, Art. 7 N 181 and 248; RAMIN SILVAN GOHARI, Die Essential Facilities-Doktrin, *sic!* 2019, 533 et seq., 535, 539, each with further references.

¹³⁶ ALFRED FRÜH, Datenzugangsrechte, *sic!* 2018 521 et seq., 528 et seq.

5. Licences for ORD

5.1. Conclusion of a contract

Freedom of contract also includes the freedom to decide whether or not to contract with a party, the so-called **freedom to conclude**.¹³⁷

From a legal perspective, ORD providers are not obliged to conclude a licence agreement with third parties for the use of research data and are generally free to **refuse to grant a licence** if requested by a third party. In particular, they can stipulate that no licences are granted to certain third parties, e.g. companies conducting commercial research or universities from certain countries. Although certain restrictions on the freedom to conclude contracts may result from cartel law, the requirements for mandatory contracting are high and will only be met in rare cases.¹³⁸

5.2. Drafting/structuring the agreement

ORD providers are generally free to structure their licence agreements as they see fit.¹³⁹ The almost unrestricted freedom of content makes it possible to structure ORD licence agreements in such a way that they comply with the ORD concept and the FAIR principles.

From a legal perspective, it is perfectly possible to premise the granting of a licence for ORD on payment of a **licence fee**. The most likely variant will be on a one-off fee that has to be paid when the licence is issued and access to the data is granted. It is also conceivable to demand payment of a licence fee from companies, and to grant free licences to universities and other research institutions.

ORD providers are free to determine the **scope** of the **rights of use** granted under a licence. In particular, restriction of the licence to non-commercial uses is conceivable. It is also possible to impose further obligations on licensees, e.g. to impose the additional obligation to make the knowledge gained from the data or the data generated from the use of ORD freely accessible.

ORD providers should specifically state whether licensees are authorised to grant **sub-licences**. Granting such authorisation is possible but does not seem to make much sense if the ORD provider wishes to retain a certain degree of control over the use of the research data. Anyone interested in using the data can obtain a licence directly from the ORD provider at any time. Under this approach, the ORD provider knows who is authorised to use the research data.

¹³⁷ BSK ORI-MEISE/HUGUENIN, fn. 106, Art. 19/20 N 8 with reference to BGE 129 III 35, E. 6.1; Gauch/Schluep/Schmid/Emmenegger, fn. 127, para. 721 et seq., 1102 et seq.

¹³⁸ See above, D.4.

¹³⁹ See above, D.5.2.

5.3. Standard licences

Licence agreements can be freely negotiated and structured between the parties. If they avail themselves of this freedom and conclude a contract that contains specific rules for the specific case, this constitutes an **individual agreement**. In many constellations, however, standard licence agreements are used which are completely pre-formulated by one party and accepted "as is" by the other party. Such standard licence agreements are, for example, the Creative Commons licences¹⁴⁰ or the licences developed by the Open Knowledge Foundation.¹⁴¹

5.3.1. Open Database Licence

The Open Knowledge Foundation has created **three standard licences for databases**: the Open Database License (ODbL), the Open Data Commons Attribution License (ODC-By) and the Open Data Commons Public Domain Dedication and License (PDDL).¹⁴² However, these licences only cover copyrights and sui generis rights to databases.¹⁴³ Other rights, in particular legal claims arising from data protection law (if any) or from a breach of the obligation to preserve data confidentiality,¹⁴⁴ are not covered. In many cases, these licences are thus not suitable for ORD.

The **Open Data Commons Public Domain Dedication and Licence (PDDL)** permits the comprehensive **use of databases and their content**. In legal terms, this is a combination of a waiver and a licence. The PDDL covers both the copyrights and the sui generis right to the database, as well as the rights to the content of the database (Art. 2.2 PDDL). Under the PDDL, the rightsholder places the database and its contents in the **public domain** (Art. 3.1 PDDL). If this is not possible because certain countries do not permit dedication to the public domain, the rightsholders waives their copyrights and sui generis rights (Art. 3.2 PDDL). If this is likewise not possible because certain countries do not permit a waiver of copyright, the rightsholders grant a comprehensive licence to the database and its content (Art. 3.3 PDDL). The PDDL does not impose any restrictions on licence holders when they use the database.

The **Open Data Commons Attribution Licence (ODC-By)** permits the **use of databases** that are protected by copyright or by the sui generis right for databases (Art. 2.1 et seq. ODC-By). However, it only relates to the rights to the databases, **not** to any rights to the **contents of databases**, in particular to any copyrights or ancillary copyrights to works or services contained in the database. Claims arising from data protection or personality rights are also not covered by the licence (Art. 2.4 ODC-By). The

¹⁴⁰ See also <<https://www.creativecommons.ch>> (last visited on 28 June 2024).

¹⁴¹ See also <<https://opendatacommons.org/licenses/>> (last visited on 28 June 2024).

¹⁴² See also <<https://opendatacommons.org/licenses/>> (last visited on 28 June 2024).

¹⁴³ See above, B.1.2. and B.1.3.

¹⁴⁴ See above, B.3 and B.1.5.

ODC-By only contains an **attribution** obligation (Art. 4.3 ODC-By). The granting of **sub-licences** is prohibited (Art. 4.4 sentence 1 ODC-By). Instead, the licensor offers to grant an ODbL to third parties who have received the database (or parts thereof) distributed under the licence in modified or unmodified form from the licensee (Art. 4.4 sentence 2 ODC-By).

The **Open Database Licence (ODbL)** contains some of the same specifications as the ODC-By, but provides for further restrictions. Like the ODC-By, the ODbL permits the **use of databases** (Art. 2.1 et seq. ODbL). Like the ODC-By, however, it only refers to the rights to the databases, not to any rights to the contents of databases (Art. 2.4 ODbL). In addition to the duty of **attribution** (Art. 4.3 ODbL), the ODbL contains an obligation to **share alike** (Art. 4.4 ODbL). The ODbL also stipulates that databases must be **kept open** (Art. 4.7.a ODbL). Third parties may protect a database which they are authorised to use in accordance with the ODbL against access and use by third parties by means of terms of use or technical measures, but only if they simultaneously make a restriction-free copy of the database available to the recipient of the database associated with such restrictions, so-called parallel distribution (Art. 4.7.b ODbL). As with the ODC-By, the granting of **sub-licences** is also prohibited under the ODbL (Art. 4.8 ODbL).

5.3.2. Creative Commons licences

Creative Commons licences are an effective tool for easily defining the scope of rights granted to users in relation to a copyrighted work. Creative Commons licences have achieved a high level of acceptance, and their use is recommended by many public institutions.¹⁴⁵ Rightsholders can determine how their content is used by choosing from six Creative Commons licence categories.

The most permissive licence is the **Attribution licence (CC BY)**. It offers users the freedom to reuse the data, provided they name the original owners and state whether any changes have been made to the original content. The **Share-Alike licence (CC BY-SA)** requires the indication of the source and the use of a newly created work based on an existing work under the same licence. The **Non-Commercial licence (CC BY-NC)** provides the same rights as the Attribution licence (CC-BY), but excludes any use for commercial purposes. The **No Derivatives licence (CC BY-ND)** permits commercial use, but prohibits any modification of derivative works.

The **Creative Commons Zero licence (CC0)** is a combination of a disclaimer and a licence. With the CC0, the affirmer gives a **comprehensive waiver** of his copyrights and similar rights (Art. 2 CC0).

¹⁴⁵ See, for example, the recommendations of the Open Access Infrastructure for Research in Europe (Open-AIRE), available at <<https://zenodo.org/record/2574619>> (last visited on 27 May 2024), which recommends the use of Creative Commons CC BY 4.0 licences if the material constitutes a work within the meaning of the CopA, and the use of the CC0 licence for data and datasets that are not structured as databases.

These rights are defined comprehensively in the CC0; they include (but are not limited to): rights of use under copyright law, moral rights, personality rights, claims arising from unfair competition law, sui generis database rights and similar rights (Art. 1 CC0). If this waiver is not valid, the affirmer grants a comprehensive, free and irrevocable licence to use all rights (Art. 3 CC0). Data published under a CC0 licence can therefore be used, modified and reused freely and without restrictions. The CC0 is an effective instrument for creating legal certainty because it makes it clear that **content** labelled with it **may be used freely**. It also has the advantage that it solves the problem of attribution stacking, i.e. the need to name a large number of reused data records. The use of a CC0 licence gives users the opportunity to combine several data sets without having to worry about naming the individual rightsholders.

5.3.3. *Enforcement*

Licence agreements are always concluded between one (or more) licensor(s) and one (or more) licensee(s). The licensor is the holder of the rights that may be used by the licensee within the scope of and on the basis of the licence agreement. If the licensee does not comply with the provisions of the licence agreement, the licensor can enforce his or her contractual rights against the licensee. Licence agreements sometimes contain provisions on the enforcement of rights, e.g. on cancellation or termination in the event of breach of contract; if these issues are not covered by the parties' agreement, the general provisions on breach of contract (Art. 97 et seq. CO and Art. 192 et seq. and Art. 367 et seq. CO by analogy) apply. This applies to both individual and standard licence agreements. As the use of the **Creative Commons licences CC-BY and CC0** is proposed for making research data accessible as ORD, the enforcement of only these two licences is briefly outlined here.

The **CC-BY licence** provides for a number of contractual duties on the part of the licensee, such as the obligation to name the author(s) or the obligation to include a copyright notice, the licence and the disclaimer of warranties (Sec. 3.a.1.A CC-BY). Furthermore, the licensee may not offer the subject matter of the licence under different or additional conditions (Sec. 2.5.B CC-BY). If a contractual obligation is breached (e.g. because the author is not named), the licence automatically terminates (Sec. 6.a CC-BY). An action for **performance of the contractual obligations** is therefore excluded because the licence agreement ends with the infringement and the former licensee can no longer be held liable for its performance once the agreement has lapsed. An action for **damages** is possible (Sec. 6.b CC-BY), but as a rule there are no damages.

Unlike the CC-BY licence, the **CC0 licence** does not impose any contractual obligations on the licensee. The licensee cannot infringe the CC0 licence, and the question of enforcing contractual claims does not arise.

The **rightsholder and licensor are entitled to enforce** the CC-BY and CC0 standard licences. According to Art. 36 of the ETH Act, the rightsholder of the ORD is the institution within the ETH Domain;



a different rule only applies to copyrights.¹⁴⁶ The respective institution within the ETH Domain is thus authorised to enforce the standard licences. If the ORD also contain works protected by copyright, a standard licence for the entirety of the data can only be granted jointly by the institution and the copyright holders. However, the two (or more) licensors can take independent action against a breach of contract and claim their proportionate share of any damages.

¹⁴⁶ See above, B.2.



Open Research Data

Limites juridiques et options d'aménagement

Prof. Dr Florent Thouvenin

Dr Stephanie Volz

Avec la collaboration de :
MLaw Deborah De Col, RA et
MLaw Samuel Mätzler, RA

Zurich, 24 mars 2025

La version originale est la version allemande. Traduction par Architext
Zürich.



Table des matières

A.	Introduction	5
1.	Mission	5
2.	Terminologie	5
B.	Principes de base	6
1.	Droits sur les données	6
1.1.	Pas de propriété de données	6
1.2.	Droit d'auteur	7
1.3.	Le droit <i>sui generis</i> des bases de données dans l'UE	10
1.4.	La reprise directe de résultats de travail (article 5 let. c LCD)	12
1.5.	Protection de secrets de fabrication et d'affaires (<i>know-how</i>)	13
2.	Statut du titulaire du droit	17
3.	Droit de la protection des données	19
C.	Limites pour les ORD	21
1.	Problématique et Approche	21
2.	Limites légales	22
2.1.	Contrôle des exportations	22
2.2.	Droit de la sécurité de l'information	24
2.3.	Droit de la santé	26
2.3.1.	Généralités	26
2.3.2.	Recherche dans le domaine humain	26
2.3.3.	Recherche dans le domaine non humain	29
2.3.4.	D'autres règles	30
2.4.	Génie génétique	31
2.5.	Droit de l'environnement	31
2.6.	Droit de produits chimiques	33
2.7.	Droit des denrées alimentaires	33
2.8.	Droit de l'énergie et de l'énergie nucléaire	34
2.9.	Droit de la protection animale	35
2.10.	Droit des marchés financiers	36
3.	Droit des tiers	37
3.1.	Droits d'auteur	37
3.2.	Brevets	38
3.3.	Droits découlant de la protection du secret par le droit pénal	39
3.4.	Droits découlant de la LCD	39
3.5.	Droits issus de la protection des données	40
4.	Restrictions contractuelles	41
5.	Responsabilité	43



D.	Mise en œuvre juridique des <i>ORD</i>	43
1.	Remarque préliminaire	43
2.	Cadre constitutionnel	44
2.1.	Droits fondamentaux pertinents pour les <i>ORD</i>	44
2.2.	Restriction des droits fondamentaux	45
3.	Contrats de licence	46
3.1.	Objet	46
3.2.	Forme	46
3.3.	Contenu	47
4.	Aspects du droit des cartels	48
5.	Licences pour les <i>ORD</i>	49
5.1.	Conclusion	49
5.2.	Rédaction	50
5.3.	Licenses standard	50
5.3.1.	Open Database License	51
5.3.2.	License Creative Commons	52
5.3.3.	Mise en œuvre	53



EXECUTIVE SUMMARY

Les droits sur les données créées dans le cadre de l'activité professionnelle des employés d'une institution du domaine des EPF appartiennent à l'institution concernée. Il n'en va différemment que pour les droits d'auteur relatifs à des œuvres littéraires et artistiques représentées dans les données. Ainsi, les institutions peuvent en règle générale déterminer comment et sous quelle forme les données doivent être rendues accessibles en tant qu'*ORD*. Toutefois, les *ORD* sont soumises à certaines limites. Celles-ci peuvent émaner de dispositions légales, de droits de tiers ou de conventions contractuelles.

L'analyse des éventuelles limites légales a montré que notamment – sans prétendre à l'exhaustivité – le droit du contrôle des exportations, le droit de la sécurité d'information, le droit de la santé, le droit du génie génétique, le droit de l'environnement, le droit des produits chimiques, le droit des denrées alimentaires, le droit de l'énergie et de l'énergie nucléaire ainsi que le droit des marchés financiers contiennent des dispositions qui pourraient s'opposer à ce que les données de recherche soient rendues accessibles en tant qu'*ORD*. Au-delà des limites légales, il convient de prendre en compte les droits éventuels de tiers. À cet égard, il s'agit notamment de droits d'auteurs, par exemple au regard d'éléments d'un jeu de données protégés par le droit d'auteur ou de certaines bases de données, ainsi que de droits issus de la protection des secrets de fabrication et d'affaires (article 162 CP et article 6 LCD), de la loi sur la concurrence déloyale (article 5 let. c LCD) et de dispositions du droit de la protection des données.

En outre, des contrats conclus avec d'autres universités ou entreprises peuvent contenir des obligations relatives au traitement des données, notamment des obligations de confidentialité, qui doivent être respectées dans le cadre des *ORD*.

La mise en œuvre d'une stratégie relative aux *ORD* doit se conformer au cadre constitutionnel. Une obligation légale de rendre les données accessibles au public peut impacter et dans certains cas enfreindre la liberté de la science, la garantie de la propriété et la liberté économique. Par ailleurs, les dispositions du droit des cartels peuvent être pertinentes, notamment au regard des obligations d'accès et d'une fixation éventuelle des prix.

En principe, les fournisseurs d'*ORD* sont libres sur le plan juridique lors de la rédaction de contrats de licence permettant à des tiers d'utiliser les données. Dans des accords individuels, ils peuvent imposer aux preneurs de licence des obligations, par exemple le paiement d'une redevance. Mais en règle générale, il sera judicieux d'utiliser des licences standard, notamment la *Creative Commons Zero License (CC0)* ou la *Creative Commons Attribution License (CC-BY)*.



A. INTRODUCTION

1. Mission

Le domaine des EPF compte six institutions indépendantes : l'École polytechnique fédérale Zurich (EPF Zurich), l'École polytechnique fédérale Lausanne (EPFL), l'Institut Paul Scherrer (IPS), le Laboratoire fédéral d'essai des matériaux et de recherche (LFEM), l'Institut fédéral de recherches sur la forêt, la neige et le paysage (FNP) et l'Institut fédéral pour l'aménagement, l'épuration et la protection des eaux (IFAEPE). Les deux écoles (EPF et EPFL) et les quatre instituts de recherche (IPS, LFEM, FNP et IFAEPE) du domaine des EPF sont des institutions indépendantes avec des personnalités juridiques distinctes. Leur activité est régie par le droit fédéral.

En mai 2020, le conseil des EPF a adopté une *Open Research Data Position of the EPF Domain* et fondé un *Open Research Data Program*. Ce programme comprend cinq mesures. La quatrième mesure concerne les fondements juridiques pour les données de recherche ouvertes (*Open Research Data (ORD)*). Dans le cadre de cette mesure, trois objectifs sont poursuivis :

- identification des obstacles juridiques (fédéraux) lors de la mise à disposition de données de recherche en tant qu'*ORD* par les chercheurs ou les institutions du domaine des EPF ;
- clarification des responsabilités des chercheurs et institutions du domaine des EPF ;
- développement de lignes directrices relatives aux *ORD* qui peuvent être utilisées dans le domaine des EPF comme référence commune.

Fin 2023, le *Center for Information Technology, Society, and Law* (ITSL) de l'Université Zurich a été mandaté par le FNP afin de conduire des travaux pour la mise en œuvre de la quatrième mesure. Ce rapport examine les questions issues des deux premiers objectifs de la quatrième mesure. Le rapport se limite au droit fédéral suisse ; la seule exception est le droit dit « *sui generis* » pour les bases de données de l'UE. L'examen se concentre sur les données matérielles. Mais comme il n'est pas toujours possible d'établir une séparation claire entre les données personnelles et matérielles, des questions relatives au droit de la protection des données sont également prises en compte. À cet égard, les explications relatives au droit de la protection des données se limitent à la loi suisse sur la protection des données (LPD), les dispositions du Règlement général sur la protection des données (RGPD) de l'UE n'étant pas examinées.

2. Terminologie

Ce rapport repose sur les définitions suivantes :

- **Données de recherche** : il s'agit de toutes les données considérées nécessaires par la communauté scientifique pertinente afin de valider les résultats de recherche. Ces données peuvent (et sont destinées à) être utilisées dans d'autres projets de recherche. Le terme recouvre des données brutes, des données traitées et des métadonnées. Étant donné que l'ordre juridique ne fait pas de distinction générale entre ces types de données, mais uniquement au sein de quelques actes législatifs, seul le terme plus large de données de recherche sera utilisé dans ce rapport.
- **Les principes FAIR** : ce sont des lignes directrices reconnues au niveau international visant à améliorer la facilité de recherche, l'accessibilité, l'interopérabilité et la réutilisation de contenus numériques.
- **Open Research Data (ORD)** : il s'agit de données de recherche qui correspondent aux principes FAIR et qui sont publiquement disponibles, accessibles et réutilisables pendant au moins dix ans. Par principe, le code source n'est pas couvert par ce terme. Il n'en va autrement que lorsque les données de recherche ne peuvent être utilisées sans le code source (spécifique) pour la validation de résultats de recherche ou pour la réutilisation dans d'autres projets de recherche. En outre, il faut noter qu'une séparation claire entre les données de recherche et le code source n'est pas toujours possible. À titre d'exemple, les *weights* (poids) dans les réseaux neuronaux profonds (*Deep Neural Networks*) entraînés peuvent être considérés comme étant du code ou des données.

B. PRINCIPES DE BASE

1. Droits sur les données

1.1. Pas de propriété de données

La question de savoir si, et sous quelles conditions, les données de recherche peuvent être rendues librement accessibles, dépend fondamentalement de la question de savoir si les données « appartiennent à quelqu'un », c'est-à-dire si des droits de propriété sur les données existent. Si la question est posée en ces termes, il peut y être répondu clairement : il n'y a **pas de propriété de données** en droit suisse, ni de données matérielles ni de données personnelles¹. La propriété selon son acception en droit des biens n'existe que pour les choses. Une chose est un objet corporel, délimité,

¹ ROLF H. WEBER/FLORENT THOUVENIN, Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft? ZRS 2018, 43 ss., 49 ; ALAIN SCHMID/KIRSTEN JOHANNA SCHMIDT/ZECH HERBERT, Rechte an Daten – zum Stand der Diskussion, sic! 2018, 627 ss., 629 ; STEPHAN WOLF/WOLFGANG WIEGAND, in : Geiser/Wolf (Ed.), Basler Kommentar Zivilgesetzbuch II, art. 457-977 ZGB et art. 1-61 SchlT ZGB, Bâle 2023, avant art. 641 ss. N 19c.

accessible au contrôle humain². Il manque le caractère corporel aux données, puisqu'elles ne sont pas saisissables. À titre d'exemple, un support de données est une chose, mais cela n'est pas le cas des données qui y sont stockées.

Le fait qu'il n'existe pas de « propriété des données » ne signifie pas pour autant que **les données** ne peuvent pas faire l'objet **d'autres droits** qui s'opposeraient à une utilisation ou à une libre mise à disposition de données. De telles restrictions peuvent résulter notamment du droit d'auteur, de la protection de secrets de fabrication et d'affaires, du droit de la protection des données et, dans l'UE, également de la protection dite « *sui generis* » des bases de données³.

En outre, il est possible d'exercer un **contrôle effectif sur les données**. Ce contrôle peut, par exemple, être exercé par le stockage dans des systèmes propriétaires ou par le cryptage. Il est également possible que le contrôle sur les données soit attribué contractuellement à l'une ou à l'autre partie. Dans ces cas on parle parfois de « *data ownership* ». Ce terme peut aider à exprimer le contrôle effectif. Mais il ne doit pas induire en erreur sur le fait que ce « *ownership* » n'est pas une propriété au sens juridique du terme. Néanmoins, ce contrôle effectif est parfois juridiquement protégé, notamment par la protection de secrets industriels et d'affaires (article 162 CP et article 6 LCD)⁴.

1.2. Droit d'auteur

Le droit d'auteur protège les **œuvres littéraires et artistiques** (article 2 al. 1 LDA). Il s'agit, entre autres, de textes, d'œuvres musicales, d'œuvres cinématographiques, d'images, d'œuvres d'architecture, de photographies et d'œuvres à contenu scientifique telles que les dessins, les plans, les cartes ou les ouvrages sculptés ou modelés (article 2 al. 2 LDA). Les **programmes d'ordinateur** sont également considérés comme des œuvres (article 2 al. 3 LDA). Les **données ne constituent pas d'œuvres littéraires et artistiques** et de ce fait elles ne sont pas en tant que telles protégées par le droit d'auteur. En revanche, lorsqu'une **œuvre littéraire et artistique** est stockée sur un support de données et est donc **représentée sous forme de données**, la protection par le droit d'auteur de l'œuvre s'étend aussi à sa représentation sous forme de données. Le droit d'auteur ne protège les œuvres que s'il s'agit de **créations de l'esprit** ayant un **caractère individuel** (article 2 al. 1 LDA). Il existe une exception pour des photographies qui sont également protégées lorsqu'elles sont dépourvues de caractère individuel (article 2 al. 3^{bis} LDA). En outre, **certaines prestations** sont protégées par les droits dits « voisins ». Une telle protection existe pour des prestations par les artistes interprètes (article 33 ss. LDA), tels que les musiciens, les artistes et les chefs d'orchestre, pour les producteurs de phonogrammes ou de

² BSK ZGB II-WOLF/WIEGAND, nbp. 1, avant art. 641 ss. N 5 ss. ; BARBARA GRAHAM-SIEGENTHALER, in : Aebi-Müller/Müller (Ed.), Berner Kommentar, Das Eigentum – Allgemeine Bestimmungen – art. 641-654a ZGB, Bern 2022, Zweiter Abschnitt Sachen und andere Rechtsobjekte N 243.

³ cf. ci-après, B.1.3.

⁴ cf. ci-après, B.1.5.

vidéogrammes (article 36 LDA) et pour les organismes de diffusion (article 37 LDA). Ces droits voisins protègent les prestations, phonogrammes ou émissions contre leur utilisation par des tiers.

La **condition de protection de la création de l'esprit** exprime l'idée que seulement les créations humaines peuvent être une œuvre au sens du droit d'auteur⁵. Les œuvres générées de façon autonome par les ordinateurs ne sont donc pas protégées, alors que les œuvres créées par les êtres humains à l'aide d'un ordinateur comme outil le sont⁶. Les œuvres, générées de façon autonome par des systèmes dits d'intelligence artificielle (IA) générative à partir d'une saisie effectuée par un être humain (appelé « *prompt* »), ne sont donc pas protégées par le droit d'auteur⁷. Il en va autrement si l'IA est utilisée comme outil afin de transposer les décisions créatrices d'un être humain. La distinction entre une création d'œuvres largement autonome par un système d'IA et l'utilisation d'un tel système comme outil nécessite une appréciation au cas par cas. La condition de protection du **caractère individuel** constitue un seuil minimum qualitatif. Seules les œuvres dans lesquelles est exprimé un certain degré de créativité sont protégées par le droit d'auteur. Ainsi les œuvres protégées se distinguent des créations banales et des simples travaux de routine. Le caractère individuel résulte d'une diversité de décisions prises par l'auteur et de combinaisons surprenantes et inhabituelles, lesquelles mènent à conclure qu'il semble exclu qu'un tiers confronté à la même tâche aurait créé une œuvre identique ou essentiellement identique⁸.

Les **programmes d'ordinateur** sont également considérés comme des œuvres (article 2 al. 3 LDA). C'est le code source qui est protégé par le droit d'auteur, à condition qu'il ait un caractère individuel. Selon la doctrine, tel est le cas lorsque le programme est nouveau et qu'il n'est pas banal ni ordinaire⁹. Toutefois, comme pour les œuvres littéraires et artistiques, il conviendrait également de déterminer pour les programmes d'ordinateur s'il semble exclu qu'un tiers confronté à la même tâche aurait créé une œuvre identique ou essentiellement identique. Cependant, lors de l'utilisation, il ne devrait pas y avoir de différences par rapport au test pour savoir si le programme est banal ou ordinaire.

⁵ BGE 130 III 168, E. 4.5 – « Bob Marley » ; MANFRED REHBINDER/LORENZ HAAS/KAI-PETER UHLIG, in : Uhlig/Rehbinder/Haas (Ed.), Orell Füssli Kommentar, URG Urheberrechtsgesetz mit weiteren Erlassen und internationalen Abkommen, Zurich 2022 URG art. 2 N 2 ; WILLI EGLOFF, in : Barrelet/Egloff (Ed.), Das neue Urheberrecht, Kommentar zum Bundesgesetz über das Urheberrecht (URG) und verwandte Schutzrechte, Kommentar, Bern 2020, art. 2 N 8 ; RETO M. HILTY, Urheberrecht, Bern 2020, para. 151.

⁶ HILTY, nbp. 5, para. 152 ; ROLAND VON BÜREN, in : von Büren/David (Ed.), Schweizerisches Immaterialgüter- und Wettbewerbsrecht (SIWR), II/2, Urheberrecht im EDV-Bereich, Bâle 1998, para. 403.

⁷ HILTY, nbp. 5, para. 152, 184 ; NATHALIE TISSOT/DANIEL KRAUS/VINCENT SALVADE, Propriété intellectuelle, Marques, brevets, droit d'auteur, Bern 2019, para. 16.

⁸ BGE 134 III 166, E. 2.3.2 – « Arzneimittel-Kompodium » ; ainsi que : BGE 142 III 387 E. 3.1 – « Fermeture d'une Terrasse » ; BGE 136 III 225, E. 4.2 – « Guide orange ».

⁹ URG Komm.-EGLOFF, nbp. 5, art. 2 N 33 et les références citées ; OFK URG-REHBINDER/HAAS/UHLIG, nbp. 5, art. 2 N 31 ; WILLI EGLOFF, FAIR Works – Eckpunkte eines Urheberrechts für digitale Welt, sic! 2022, 405 ss., 412.

Les **recueils** sont également protégés par le droit d'auteur s'ils remplissent les conditions de protection du droit d'auteur, notamment s'ils ont un caractère individuel, en raison du choix ou de la disposition de leur contenu (article 4 al. 1 LDA). Les **bases de données** sont également considérées comme des recueils. Les bases de données sont protégées si elles ont un caractère individuel, en raison du choix ou de la disposition des données qui y sont contenues¹⁰. Pour les bases de données, il n'est pas simple de remplir cette condition. En règle générale, seules des bases de données structurées sont protégées par le droit d'auteur puisque dans le cas des bases de données non structurées la disposition des données pouvant justifier la protection par le droit d'auteur fait défaut¹¹. Le choix des données à lui seul ne devrait quasiment jamais avoir un caractère individuel pouvant ainsi justifier la protection par le droit d'auteur. Une protection éventuelle des bases de données par le droit d'auteur n'a toujours trait qu'au choix et à la disposition des données, pour ainsi dire à la **structure de la base de données**, et non aux données en tant que telles. Les données individuelles – et même l'ensemble des données – ne sont pas protégées par le droit d'auteur.

Il convient de noter que le droit d'auteur ne protège pas seulement les œuvres entières (par exemple, tout le code source), mais **aussi ses parties** (par exemple, les parties d'un texte, des séquences d'un code source ou les parties d'une base de données), si les parties remplissent à elles seules les conditions de protection, notamment si elles ont un caractère individuel (article 2 al. 4 LDA).

Les titulaires des droits d'auteurs ont le droit exclusif de décider si, quand et de quelle manière l'œuvre sera utilisée (article 10 al. 1 LDA). Une partie de ce droit d'utilisation est ce que l'on appelle le **droit de mise à disposition**, c'est-à-dire le droit, de mettre l'œuvre à disposition, de manière que chacun puisse y avoir accès de l'endroit et au moment qu'il choisit individuellement (article 10 al. 2 let. c LDA). Ce droit comprend la mise à disposition de l'œuvre par Internet. Les œuvres protégées par le droit d'auteur ne doivent donc être mises à disposition en tant qu'**ORD** qu'avec l'accord du titulaire des droits.

L'utilisation d'œuvres protégées par le droit d'auteur dans le cadre de la recherche est toutefois largement autorisée par le biais de **limites**. L'utilisation d'œuvres pour la recherche personnelle (par exemple, la rédaction d'une thèse) est autorisée par la limite de l'usage privé (article 19 al. 1 let. a LDA)¹². La reproduction d'œuvres pour la recherche au sein d'une organisation peut être qualifiée d'usage en entreprise et est ainsi également autorisée (article 19 al. 1 let. c LDA)¹³. En outre, la LDA contient une limite explicite en faveur de la recherche scientifique permettant de reproduire des œuvres

¹⁰ EGLOFF, nbp. 5, URG 4 N 6 ; HILTY, Urheberrecht, para. 249 ; IVAN CHERPILLOD, in : Müller/Oertli (Ed.), Stämpfli Handkommentar, Urheberrechtsgesetz (URG), Bundesgesetz über das Urheberrecht und verwandte Schutzrechte. Mit Ausblick auf EU-Recht, deutsches Recht, Staatsverträge und die internationale Rechtsentwicklung, Bern 2012, art. 4 N 4.

¹¹ CJUE GRUR 2009, 572 ; OGer ZH du 1^{er} septembre 1992, in : SMI 1993, 331 ss. ; URG Komm.-EGLOFF, nbp. 5, art. 4 N 6 et les références citées.

¹² BARRELET/EGLOFF, nbp. 5, art. 19 N 11 ; SHK URG-Gasser, nbp. 10, art. 19 N 21.

¹³ BARRELET/EGLOFF, nbp. 5, art. 19 N 20 ; OFK URG-REHBINDER/HAAS/UHLIG, nbp. 5, art. 19 N 31.

à des fins de recherche scientifique, si la reproduction est conditionnée par l'utilisation d'un procédé technique et s'il existe un accès licite aux œuvres à reproduire (article 24d al. 1 LDA). Les citations tirées d'œuvres sont en outre autorisées par la limite de la liberté de citation (article 25 LDA). Si les conditions de l'une de ces limites sont remplies, les œuvres et prestations protégées peuvent aussi, sans l'accord des titulaires des droits d'auteur et des droits voisins, être utilisées dans le cadre de la recherche et notamment être reproduites, c'est-à-dire, par exemple, être stockées sur un serveur. Cependant, ces limites ne permettent pas de mettre des œuvres à disposition en tant qu'*ORD* sur une plateforme.

La **protection** par le droit d'auteur est **limitée dans le temps**. Pour les œuvres littéraires et artistiques, elle prend fin soixante-dix ans après le décès de l'auteur, et pour les programmes d'ordinateur, cette protection expire cinquante ans après. Pour les photographies dépourvues de caractère individuel, la protection prend fin cinquante ans après la confection (article 29 ss. LDA). La protection des prestations d'artistes interprètes prend fin soixante-dix ans après la prestation, la protection de producteurs de phonogrammes ou vidéogrammes après la confection du support. La protection de prestations d'une entreprise de radiodiffusion prend fin cinquante ans après la diffusion de l'émission (article 39 LDA). Après l'expiration de la protection, les œuvres et prestations tombent dans le **domaine public (*public domain*)** et peuvent être utilisées librement, c'est-à-dire qu'elles peuvent, par exemple, être mises à disposition en tant qu'*ORD*.

1.3. Le droit *sui generis* des bases de données dans l'UE

Avec la **Directive 96/9/CE concernant la protection juridique des bases de données** (directive sur les bases de données), la Communauté européenne (CE) de l'époque a créé au milieu des années 1990 une protection spéciale pour les bases de données. Avec la transposition de la directive concernant la protection juridique des bases de données, les États membres de la CE ont créé dans leur droit national une *protection* des bases de données *par le droit d'auteur* ainsi qu'un droit dit « *sui generis* » pour les fabricants des bases de données¹⁴. La création et la durée de la protection par le droit d'auteur des bases de données sont déterminées par le droit d'auteur. Le droit *sui generis* est créé avec l'achèvement de la fabrication et prend fin après quinze ans (article 10 al. 1 directive sur les bases de données).

Le **droit suisse ne connaît pas de droit *sui generis***, seulement une protection des bases de données par le droit d'auteur¹⁵. Par conséquent, en Suisse, les bases de données ne sont pas protégées contre l'extraction et/ou la réutilisation des données qui y sont contenues. Néanmoins, il convient de respecter

¹⁴ art. 7 ss. Directive sur les bases de données ; pour la motivation, voir notamment le considérant 38 de la Directive sur les bases de données.

¹⁵ cf. supra, B.1.2.

le droit *sui generis* des bases de données lors de la mise à disposition de données de recherche en tant qu'*ORD*, puisque les données sont rendues disponibles au niveau mondial (et donc dans l'UE) et chaque type de mise à disposition publique de données est considérée comme une réutilisation. La mise à disposition de données en tant qu'*ORD* peut donc enfreindre le droit *sui generis* des bases de données – indépendamment du lieu du serveur.

La finalité du droit *sui generis* sur les bases de données est de protéger les investissements des fabricants des bases de données¹⁶. On entend par « base de données » un recueil d'œuvres, de données ou d'autres éléments indépendants¹⁷, **disposés de manière systématique ou méthodique** et individuellement accessibles par des moyens électroniques ou d'une autre manière (article 1 al. 2 directive sur les bases de données)¹⁸. La protection ne couvre donc que des bases de données structurées, et non des recueils de données non structurées¹⁹. La condition pour la protection est que le fabricant ait effectué qualitativement et quantitativement un investissement substantiel dans l'obtention, la vérification ou la présentation du contenu d'une base de données. Seuls les moyens mis en œuvre afin de rechercher et de rassembler des éléments sont considérés comme un investissement relatif à la base de données, et non l'investissement dans la création de ces éléments, c'est-à-dire les données en tant que telles²⁰.

Le droit *sui generis* confère à son titulaire le droit d'interdire l'extraction et/ou la réutilisation de la totalité ou d'une partie substantielle, évaluée de façon qualitative ou quantitative, du contenu de celle-ci²¹. Par « **extraction** », on entend le transfert permanent ou temporaire du contenu d'une base de données sur un autre support par quelque moyen ou sous quelque forme que ce soit (article 7 al. 2 let. a directive sur les bases de données). Par « **réutilisation** », on entend toute forme de mise à disposition du public (article 7 al. 2 let. b directive sur les bases de données)²². On peut considérer qu'il s'agit d'une « partie substantielle » lorsque par rapport au contenu total de la base de données une partie quantitativement importante est extraite et/ou réutilisée. Il s'agit d'une partie qualitativement substantielle lorsque

¹⁶ CJUE du 9 octobre 2008, C-304/07 – Directmedia vs. Albert-Ludwigs-Universität, para. 33 ; CJUE du 19 décembre 2013, C-202/12, Innoweb vs. Wegener, para. 36 ss.

¹⁷ CJUE du 29 octobre 2015, C-490/14 – Freistaat Bayern vs. Verlag Esterbauer GmbH, para. 17 et 22.

¹⁸ Selon la CJUE il doit être possible de « localiser tout élément indépendant contenu en son sein », par ex., par un moyen technique, un index, une table des matières etc. ; CJUE du 9 novembre 2004, C-444/2 – Fixtures Marketing vs. OPAP, para. 30.

¹⁹ CJUE du 1^{er} mars 2012, C-604/10, para. 30 et 32 – Football Dataco vs. Yahoo!.

²⁰ CJUE du 9 novembre 2004, C-203/02 – British Horseracing vs. Hill Organization, para. 38 ; CJUE du 9 novembre 2004, C-444/2 – Fixtures Marketing vs. OPAP, para. 39 ss., not. 47 ; FLORENT THOUVENIN, Funktionale Systematisierung von Wettbewerbsrecht (LCD) und Immaterialgüterrecht, Diss. Zurich, Köln/Berlin/München 2007, 392.

²¹ THOUVENIN, nbp. 20, 393.

²² Selon la CJUE les notions « extraction », et « réutilisation » comprennent toutes les utilisations non autorisées, qui portent atteinte à l'investissement de la personne qui a constitué cette base ; CJUE du 9 novembre 2004, C-203/02 – British Horseracing vs. Hill Organization, para. 51 ; Heiko SENDROWSKI, Zum Schutzrecht «sui generis» an Datenbanken, GRUR 2005, 369 ss., 374.

l'investissement effectué pour le ou les élément(s) extrait(s) est important par rapport à l'investissement effectué dans l'intégralité de la base de données²³. L'extraction et la réutilisation de parties non substantielles ne sont pas non plus autorisées si elles sont répétées et systématiques et contraires à une exploitation normale de cette base de données par le fabricant, ou si elles causent un préjudice injustifié aux intérêts de celui-ci (article 7 al. 5 directive sur les bases de données).

Alors que le droit d'auteur protège le choix et la disposition des données dans une base de données, et donc leur structure²⁴, le droit *sui generis* protège le **contenu des bases de données**, c'est-à-dire une majorité de données, en prenant en compte l'extraction d'éléments individuels ou de plusieurs éléments à partir d'une base de données, indépendamment du fait que la structure de la base de données ait également été reprise²⁵. Le fabricant d'une base de données peut ainsi interdire aux tiers d'extraire ou de réutiliser sous quelque forme que ce soit, les données qui y sont contenues à condition qu'il s'agisse de parties quantitativement ou qualitativement substantielles. Certes, le droit *sui generis* confère ainsi des droits exclusifs sur le contenu des bases de données et sur certains volumes de données, mais pas sur les données individuelles contenues dans les bases de données.

1.4. La reprise directe de résultats de travail (article 5 let. c LCD)

La LCD ne prévoit pas seulement la protection de secrets de fabrication et d'affaires, mais également la protection contre la reprise directe de résultats de travail. Selon l'article 5 let. c LCD, agit de façon déloyale la personne qui reprend grâce à des procédés techniques de reproduction et sans sacrifice correspondant le résultat du travail d'un tiers, prêt à être mis sur le marché, et l'exploite comme tel. Cette protection s'étend également à la reprise directe de données et peut donc avoir des effets similaires au droit *sui generis* sur les bases de données²⁶.

Selon la doctrine et la jurisprudence, un **résultat de travail prêt à être mis sur le marché** est constitué par un produit qui peut être exploité de façon commerciale sans intervention supplémentaire²⁷. Ce résultat de travail doit être matérialisé d'une façon ou d'une autre, parce qu'autrement il ne pourrait pas être repris par un procédé de reproduction technique²⁸. Il peut s'agir non seulement de résultats de

²³ CJUE du 5 mars 2009, C-545/07 – Apis-Hristovich vs. Lakorda, para. 56 ss., not. 59, 66 et 74 ; SENDROWSKI, nbp. 22, 375 ; ANDREAS WIEBE, Schutz von Maschinendaten durch das sui-generis-Schutzrecht für Datenbanken, GRUR 2017, 338 ss., 343 ss.

²⁴ Considérants 15 et 39 Directive sur les bases de données.

²⁵ Voir aussi considérant 58 Directive sur les bases de données, selon lequel le droit d'auteur protège la structure, et en revanche le droit *sui-generis* le contenu ; CJUE du 5 mars 2009, C-545/07 – Apis-Hristovich vs. Lakorda, para. 55.

²⁶ cf. supra, B.1.3.

²⁷ FLORENT THOUVENIN, art. 5 let. c LCD – reloaded, sic! 2018, 595 ss., 598 ; BGE 131 III 384, 389 – « Suchspider ».

²⁸ BGE 131 III 384, 389 – « Suchspider » ; ähnlich auch ROLF H. WEBER/LENNART CHROBAK, in : Heizmann/Loacker (Ed.), Kommentar zum Bundesgesetz gegen den unlauteren Wettbewerb (UWG), Zurich/St. Gallen 2018, art. 5 let. c N 19.

travail matériels, mais également de résultats de travail immatériels, tels que des enregistrements de son et d'images, des programmes d'ordinateur ou des données qui sont stockées sur un support de données²⁹. Le critère de **procédé de reproduction technique** n'a pas été défini de façon précise ni par le législateur ni par la doctrine et la jurisprudence. Toutefois, des procédés de reproduction numériques, tels que le *web scraping* ou la création de copies numériques de données³⁰, sont à qualifier sans aucun doute de procédés de reproduction techniques. Par « **reprise** », on entend une reproduction consistant à intégrer l'objet du résultat de travail dans le procédé de reproduction³¹, par « **exploitation** », toute application commerciale ou usage professionnel dans le cadre d'une activité économique³². En premier lieu, on entend par là l'utilisation du résultat de travail repris pour la fabrication d'un produit concurrent. Toutefois, selon une partie de la doctrine et la jurisprudence il suffirait que le résultat de travail soit utilisé comme base d'une prestation propre³³.

Le législateur a délibérément formulé de façon ouverte le critère de **sacrifice correspondant**. Il doit permettre de « jauger l'avantage injustifié dont jouit le second concurrent » et de tenir compte de l'amortissement « du sacrifice fait par le premier concurrent pour créer le produit repris »³⁴. Il est communément admis que le sacrifice correspondant doit être déterminé dans le cadre d'une « double comparaison du sacrifice »³⁵.

Certes, il ne peut être répondu à la question de savoir si les conditions de l'article 5 let. c LCD sont remplies qu'au cas par cas. Mais la disposition montre que la reprise de données de tiers peut également enfreindre une disposition de la LCD lorsque ces données ne sont pas tenues secrètes mais sont accessibles au public.

1.5. Protection de secrets de fabrication et d'affaires (*know-how*)

Les secrets de fabrication et d'affaires ne sont certes pas protégés par les droits sur les biens immatériels, mais les secrets sont protégés par une série de normes contre la divulgation et l'utilisation par des tiers. Ces dispositions sanctionnent, si les conditions sont réunies, les **atteintes au contrôle**

²⁹ BGE 131 III 384, 389 ss. – « Suchspider » ; UWG-Komm.-WEBER/CHROBAK, nbp. 28, art. 5 let. c N 15, 18 ; SIMONE BRAUCHBAR BIRKHÄUSER, in : Jung (Ed.), Stämpflis Handkommentar, Bundesgesetz gegen den unlauteren Wettbewerb, Bern 2023, art. 5 N 23 ; RETO ARPAGAU, in : Hilty/Arpagaus (Ed.), Basler Kommentar, Bundesgesetz gegen den unlauteren Wettbewerb (UWG), Bâle 2013, art. 5 N 31, 36.

³⁰ UWG Komm.-WEBER/CHROBAK, nbp. 28, 5 N 43 ; BSK LCD-ARPAGAU, nbp. 29, 5 N 84 ; ainsi aussi SHK UWG -BRAUCHBAR BIRKHÄUSER, nbp. 29, art. 5 N 33.

³¹ UWG Komm.-WEBER/CHROBAK, nbp. 28, art. 5 let. c N 23 ; ARNAUD NUSSBAUMER, in : Martenet/Pichonnaz (Ed.), Commentaire Romand, Loi contre la concurrence déloyale (LCD), Bâle 2017, art. 5 N 68.

³² UWG Komm.-WEBER/CHROBAK, nbp. 28, art. 5 let. c N 25.

³³ BSK UWG-ARPAGAU, nbp. 29, art. 5 N 74.

³⁴ Message LCD, FF 1983 1009, 1071.

³⁵ BGE 131 III 384, E. 4.3 – « Suchspider » ; BGE 134 III 166, E. 4.3 – « Arzneimittelkompendium » ; BGE 139 IV 17, E. 1.5 – « Cardsharing » ; BSK UWG-ARPAGAU, nbp. 29, Art. 5 N 91 ; UWG Komm.-WEBER/CHROBAK, nbp. 28, art. 5 let. c N 47, 53.

effectif sur les données et servent ainsi à sécuriser le contrôle effectif des données sur le plan juridique³⁶. Il s'agit en premier lieu des dispositions des articles 6 LCD et 162 CP.

Selon l'article 6 LCD, agit de façon déloyale (et donc illégale) celui qui exploite ou divulgue des secrets de fabrication ou d'affaires qu'il a surpris ou dont il a eu indûment connaissance d'une autre manière. Par « **secret** », on entend « la connaissance particulière de faits qui ne sont pas publics ni accessibles au public, et pour lesquels le fabricant ou le détenteur du secret a un intérêt légitime à les garder secrets et qu'il souhaite effectivement garder secrets »³⁷. En outre, un tel secret doit avoir un impact potentiel sur le résultat d'affaires de l'entreprise, il doit ainsi être « pertinent pour la fabrication ou les affaires » pour être protégé par l'article 6 LCD³⁸.

Toutefois, **l'article 6 LCD** ne protège pas les secrets d'entreprise en soi, mais ne confère des droits que contre **l'exploitation et la divulgation de secrets**, après que la connaissance de ceux-ci a été surpris ou obtenu indûment d'une autre manière³⁹. Après une telle obtention illicite de connaissances, l'article 6 LCD exige une action supplémentaire qui est objectivement susceptible d'influencer la concurrence⁴⁰. Si ces conditions sont remplies, l'ayant droit peut faire valoir ses droits prévus par la loi afin de faire interdire et faire cesser l'atteinte (article 9 al. 1 let. a et b LCD). Par ailleurs, l'article 23 al. 1 LCD sanctionne pénalement la violation de l'article 6 LCD sur plainte.

Quiconque révèle un secret de fabrication ou un secret commercial qu'il est tenu de garder en vertu d'une obligation légale ou contractuelle, quiconque utilise cette révélation à son profit ou à celui d'un tiers, est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire conformément à **l'article 162 CP**. L'infraction pénale est dans une large mesure identique à celle prévue à l'article 6 LCD, à l'exception de **l'obligation contractuelle ou légale de secret** nécessaire ici⁴¹. En ce qui concerne la terminologie, le terme de secret de fabrication et d'affaires à l'article 6 LCD est identique à celui utilisé à l'article 162 CP⁴².

³⁶ ALFRED FRÜH, Datenzuordnung und Datennutzung, digma 2019, 172 ss., 173.

³⁷ BSK UWG -FRICK, nbp. 29, art. 6 N 12 ; BGer 4A_78/2014 du 23 septembre 2014, E. 11.1 ; OGer ZH UE140269 du 19 mars 2015, E. 2.c.

³⁸ SHK UWG -MABILLARD, nbp. 29, art. 6 N 13 ; BSK UWG-FRICK, nbp. 29, art. 6 N 15, à chaque fois avec les références citées.

³⁹ BSK UWG -FRICK, nbp. 29, art. 6 N 5 ; SHK UWG-MABILLARD, art. 6 N 21.

⁴⁰ SHK UWG -MABILLARD, art. 6 N 21 ; BSK UWG -FRICK, art. 6 N 53, à chaque fois avec les références citées.

⁴¹ MARCEL ALEXANDER NIGGLI/NADINE HAGENSTEIN, in : Niggli/Wiprächtiger (Ed.), Basler Kommentar, Strafgesetzbuch und Jugendstrafgesetzbuch (StGB/JStGB), Bâle 2019, art. 162 N 52 ; SHK UWG -MABILLARD, nbp. 38, art. 6 N 5 et les références citées.

⁴² SHK UWG -MABILLARD, nbp. 38, art. 6 N 8 ; BSK UWG-FRICK, nbp. 29, art. 6 N 13 ; LORENZA FERRARI HOFER/DAVID VASELLA, in : Amstutz/Atamer (Ed.), Handkommentar zum Schweizer Privatrecht, Wirtschaftliche Nebenerlasse: FusG, UWG, KKG, PauRG und PrHG, Zurich 2023, art. 6 N 3.

La protection de secrets de fabrication et d'affaires par les articles 6 LCD et 162 CP n'est pas soumise à une durée déterminée, elle peut donc (théoriquement) durer éternellement. Toutefois, **la protection prend fin lorsque l'information n'est plus secrète**⁴³.

La question de savoir si les **données de recherche** sont protégées par l'article 6 LCD et l'article 162 CP, lorsqu'elles sont tenues secrètes, est empreinte d'incertitude. Comme cela a été exposé, la qualification comme secret de fabrication et d'affaires requiert que les faits secrets aient une certaine **valeur économique** voire que les faits secrets puissent avoir un impact sur le résultat de l'entreprise⁴⁴. Dans ce contexte, la doctrine soutient que les informations de valeur scientifique, universitaire ne sont pas des secrets au sens de l'article 6 LCD (et donc au sens de l'article 162 CP), tant qu'elles ne sont pas transférées à une entreprise⁴⁵. D'autres auteurs mentionnent des travaux de recherche et de développement (universitaires ou internes à l'entreprise) comme exemples de secrets de fabrication et d'affaires, mais également sous réserve que ces travaux soient significatifs pour le succès commercial et qu'ils aient donc une certaine pertinence économique⁴⁶. Une valeur économique devrait être aisément établie lorsque les universités génèrent des données de recherche dans le cadre de leurs activités économiques privées (missions de recherche pour des entreprises, réalisation d'expertises, etc.). Selon l'état actuel de la doctrine et la jurisprudence, il reste incertain que les données de recherche, qui ont été générées par les universités dans le cadre de la recherche « normale » et donc en principe non commerciale, aient une valeur économique au sens de l'article 6 LCD et de l'article 162 CP – et qu'elles relèvent donc de la protection de secrets selon ces dispositions.

Selon une interprétation téléologique, il conviendrait de conférer aux **données de recherche la protection de l'article 6 LCD et de l'article 162 CP**. En effet, la finalité de ces dispositions est d'empêcher des pertes économiques dues à la divulgation et l'exploitation non autorisées de secrets. Cet aspect sous-tend également la confidentialité de données de recherche universitaire. Celle-ci est censée permettre le contrôle par l'université ou les chercheurs d'un résultat de travail central et empêcher que des tiers (par exemple des entreprises ou d'autres chercheurs) obtiennent des avantages économiques (ou autres) grâce à l'utilisation des données de recherche. Dans ce contexte, il s'impose de qualifier des données de recherche universitaire de secrets d'affaires.

Par conséquent, des données de recherche peuvent certes être qualifiées de **secrets au sens de l'article 6 LCD et l'article 162 CP**. Toutefois, cela ne signifie pas que la mise à disposition de données

⁴³ SHK UWG-MABILLARD, nbp. 38, art. 6 N 19 ; BSK UWG-FRICK, nbp. 29, art. 6 N 51.

⁴⁴ En ce qui concerne le CP : ANDREAS DONATSCH, in : Orell Füssli Kommentar StGB/JStGB, avec d'autres actes législatifs et commentaire des dispositions pénales de la LCR, LStup, LEI et LAO, Zurich 2022, art. 162 N 3 ; BSK StGB-NIGGLI/HAGENSTEIN, nbp. **Error! Bookmark not defined.**, art. 162 N 9 ; STEPHAN SCHLEGEL, in : Wohlers/Godenzi/Schlegel (Ed.), Handkommentar, Schweizerisches Strafgesetzbuch, Bern 2020, art. 162 N 3.

⁴⁵ BSK UWG-FRICK, nbp. 29, art. 6 N 15.

⁴⁶ OFK StGB-DONATSCH, nbp. 44, art. 162 N 3.

de recherche en tant qu'*ORD* remplit les conditions de ces dispositions. **L'article 6 LCD** ne concerne que l'exploitation ou la divulgation de secrets que la personne concernée a surpris ou dont elle a eu indûment connaissance d'une autre manière. Cela n'est généralement pas le cas lorsque les données de recherche sont mises à disposition en tant qu'*ORD* puisque dans le cadre de leurs travaux de recherche, les chercheurs ont accès aux données ou les ont générées eux-mêmes. Il n'en va autrement que si les chercheurs ont obtenu illégalement accès aux données. Cependant, une violation de **l'article 162 CP** est possible. Cela présuppose qu'il existe une **obligation légale ou contractuelle** de garder un secret. La mise à disposition de données de recherche en tant qu'*ORD* peut se heurter à des obligations de confidentialité notamment issues de contrats conclus dans le cadre de coopérations de recherche avec des entreprises (ou d'autres institutions de recherche)⁴⁷. De tels contrats sont souvent conclus avant toute coopération proprement dite, par exemple en la forme d'accords de confidentialité (NDA) ou d'accord de transferts de matériel (MTA). Dans la pratique, ces contrats ont une grande importance. Pour les coopérations de recherche avec des entreprises (ou d'autres institutions de recherche) il est primordial que ces dispositions contractuelles soient respectées, y compris, mais pas seulement, les dispositions de confidentialité. Si les données sont divulguées en tant qu'*ORD* en violation d'une obligation contractuelle, il s'agit non seulement d'une violation du contrat, mais également d'une violation de l'article 162 CP et donc d'un fait punissable. Ce délit est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. C'est le détenteur du secret qui est habilité à déposer plainte⁴⁸.

D'autres éléments constitutifs d'infractions pénales visant à protéger les secrets se trouvent en droit suisse parmi les actes punissables commis à l'encontre des devoirs de fonction et de profession, notamment la violation **du secret de fonction** (article 320 CP). La notion de secret doit être comprise de façon similaire à celles de l'article 6 LCD et de l'article 162 CP. Toutes les informations non généralement connues ou accessibles que le détenteur souhaite protéger contre la divulgation et pour lesquelles le maintien du secret relève d'un intérêt objectif, sont également à considérer comme des secrets conformément à l'article 320 CP⁴⁹. Un secret devient un secret de fonction lorsque le fait à garder secret a été confié au titulaire de la fonction dans sa qualité de fonctionnaire ou qu'il en a eu connaissance en raison de sa fonction officielle⁵⁰. En d'autres termes, il faut un lien de causalité entre la connaissance du secret et la fonction officielle. La question de savoir si des **données de recherche universitaire** remplissent ce critère, ne semble pas avoir été discutée jusque-là dans la doctrine et/ou

⁴⁷ cf. infra, C.4.

⁴⁸ BSK StGB-NIGGLI/HAGENSTEIN, nbp. 41 **Error! Bookmark not defined.**, art. 162 N 56 f. ; OFK StGB-DONATSCH, nbp. 44, art. 162 N 8.

⁴⁹ BSK StGB-OBERHOLZER, nbp. 41, art. 320 N 8 ; OFK StGB-ISENRING, nbp. 44, art. 320 N 3, à chaque fois avec les références citées.

⁵⁰ Casuistique : Dossier de patient de la SUVA (BGE 142 IV 65, E. 5.2) ; toutes les informations relatives à une procédure pénale (BGer 6B_439/2016 du 21 avril 2017, E. 2.2.2) ; Inscriptions au casier judiciaire (BGE 127 IV 122, E. 1).

la jurisprudence. De ce fait, la norme doit être interprétée. La formulation de l'article 320 CP (« confié » et « a eu connaissance ») laisse présumer que seuls les faits secrets déjà existants sont pris en compte, dont le ou la fonctionnaire a eu connaissance dans le cadre de ses fonctions officielles. En revanche, des connaissances ou faits créés ou générés dans le cadre de l'activité officielle ne sont pas inclus. Des données de recherche, générées dans le cadre de travaux de recherche universitaire, ne sont donc pas comprises dans la notion de secret de fonction. Ce résultat est également étayé par une interprétation téléologique de cette disposition qui sert en premier lieu au maintien de secrets pour lesquels il existe un intérêt public (par exemple, la confidentialité de la stratégie de politique extérieure de la Suisse) ou un intérêt individuel (par exemple, une inscription au casier judiciaire), et dont la connaissance a été acquise dans le cadre d'une fonction officielle. Même s'il existe des constellations dans lesquelles il y a des intérêts publics ou privés à garder les données de recherche secrètes, le fait de garder les données de recherche secrètes ne sert pas (en premier lieu) à protéger les intérêts de tiers, mais à protéger les intérêts des chercheurs et des institutions de recherche dans le contrôle des données générées dans le cadre de la recherche et dans leur exploitation scientifique ou économique. Les données de recherche, générées par des institutions de recherche publiques – par exemple, les institutions du domaine des EPF – dans le cadre de leurs recherches sont donc des secrets d'affaires (au sens large) et non des secrets de fonction.

2. Statut du titulaire du droit

Dans la mesure où il existe des droits sur des données, la question se pose de savoir à qui appartiennent ces droits. Les lois relatives aux droits sur des biens immatériels ne règlent que la question de l'acquisition originale et précisent que les droits sur des biens immatériels peuvent être transférés, et donc également acquis de façon dérivée. Toutefois, ces lois (à l'exception de l'article 17 LDA) ne règlent pas la question de savoir à qui reviennent les droits sur les biens immatériels dans la relation entre employeur et salarié. En ce qui concerne la relation de travail dans le secteur privé, cette question est réglée par le droit sur les brevets et les designs à l'article 332 CO ; pour le droit d'auteur, le législateur a délibérément omis de régler cette question (sauf pour les programmes d'ordinateur à l'article 17 LDA). En ce qui concerne la relation entre les chercheurs et les institutions du domaine des EPF, la question est réglée à l'article 36 de la Loi sur les EPF.

L'article 36 al. 1 de la Loi sur les EPF est le suivant : « Tous les droits sur des biens immatériels que des personnes ayant des rapports de travail au sens de l'article 17 créent dans l'exercice de leur activité au service de leur employeur reviennent aux EPF et aux établissements de recherche ; les droits d'auteur ne sont pas concernés par cette disposition. »

Le texte de la loi et les explications dans le message précisent que la disposition s'applique à tous les biens immatériels faisant l'objet d'une réglementation spéciale, notamment aux inventions, aux œuvres littéraires et artistiques, aux designs, aux marques, aux topographies de semi-conducteurs et aux

variétés végétales⁵¹. Ni la loi ni le message ne mentionnent les droits sur les données qui ne sont pas protégées par le droit sur des biens immatériels. Le droit aux secrets d'affaires qui est au premier plan lorsqu'il s'agit de données n'est pas non plus abordé directement. Toutefois, le message clarifie que les institutions du domaine des EPF créent « dans une large mesure un savoir-faire économiquement exploitable » et que l'objectif de la révision de l'article 36 de la Loi sur les EPF est de « réglementer clairement l'ensemble des droits sur les biens immatériels dans le domaine des EPF ».

Comme indiqué, **les données ne sont pas des choses**⁵², mais **des biens immatériels**⁵³. L'article 36 de la Loi sur les EPF prévoit que « **tous les droits sur des biens immatériels** » qui ont été créés par les salariés de ces institutions dans l'exercice de leur activité au service de leur employeur reviennent aux institutions du domaine des EPF à l'exception des droits d'auteur. Aussi dans la note marginale de l'article 36 de la Loi sur les EPF ce n'est pas le terme « **droits sur des biens immatériels** » qui est employé, mais « **biens immatériels** ». La formulation de la disposition parle donc en faveur d'un champ d'application plus vaste, qui englobe tous les biens immatériels et non seulement des droits sur des biens immatériels faisant l'objet d'une réglementation spéciale – et donc également les éventuels droits sur les données.

Une interprétation téléologique de la disposition mène à la même conclusion, d'autant plus que, selon le message, le Conseil fédéral voulait instaurer « **une attribution claire des droits sur l'ensemble des biens immatériels dans le domaine des EPF** ». Le fait que l'employeur obtienne les droits sur les biens créés par ses salariés dans l'exercice de leur activité au service de leur employeur, va tellement de soi en ce qui concerne les choses que la question n'est même pas réglée en droit du travail. Une réglementation légale n'existe que pour les droits sur des biens immatériels – et la question y est toujours résolue par une attribution du droit à l'employeur, à l'exception du droit d'auteur dominé par le principe du créateur. Et même dans le droit d'auteur, la seule réglementation légale, ne s'appliquant qu'aux programmes d'ordinateur, prévoit l'attribution des droits à l'employeur (article 17 LDA). Conformément à l'article 36 al. 2 phrase 1 de la Loi sur les EPF, la même chose s'applique aux institutions du domaine des EPF.

Comme indiqué, les données ne sont protégées que partiellement et qu'indirectement par des droits sur des biens immatériels faisant l'objet d'une réglementation spéciale⁵⁴. Toutefois, elles sont couvertes par la **protection de secrets de fabrication et d'affaires** à l'article 6 LCD et à l'article 162 CP, si elles remplissent les conditions de qualification de secret⁵⁵. La protection de secrets de fabrication et

⁵¹ Message Loi sur les EPF, FF 2002 3465 ss., 3495.

⁵² cf. supra, B.1.1.

⁵³ FLORENT THOUVENIN, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, SJZ 113/2017, 21 ss., 25.

⁵⁴ cf. supra, B.1.2.

⁵⁵ cf. supra, B.1.5.

d'affaires transfère également des **droits à des informations secrètes**. Ceux-ci sont à qualifier, comme les droits sur des biens immatériels, comme des droits subjectifs⁵⁶. En *common law*, la protection de *trade secrets* est ainsi comprise comme un droit sur un bien immatériel (*intellectual property right*)⁵⁷. L'accord sur les ADPIC que la Suisse a également signé et ratifié repose également sur cette compréhension⁵⁸. Ainsi il existe des raisons tout à fait valables de qualifier les droits sur des informations secrètes que la protection de secrets de fabrication et d'affaires transfère au détenteur du secret, de droits sur des biens immatériels, d'autant plus qu'il s'agit de droits subjectifs à des biens immatériels. Il n'y a pas lieu de répondre ici à la question de savoir si ces raisons savent convaincre pour le droit suisse. Car les données sont sans doute des biens immatériels au sens de l'article 36 de la Loi sur les EPF. Les droits sur les données sont ainsi couverts par cette disposition et la propriété de ces données est attribuée aux institutions du domaine des EPF.

L'interprétation de l'article 36 de la Loi sur les EPF mène ainsi à la conclusion que les **droits sur les données** que les salariés des institutions du domaine des EPF génèrent dans l'exercice de leur activité au service de leur employeur reviennent à ces institutions.

3. Droit de la protection des données

La Loi sur la protection des données (LPD) régit le traitement des **données personnelles de personnes physiques** (article 2 al. 1 LPD). On entend par « données personnelles » toutes les informations concernant une personne physique identifiée ou identifiable (article 5 let. a LPD). La notion de données personnelles a donc un sens très large. La notion de **traitement** est également très large. Il englobe toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données (article 5 let. d LPD). La LPD a donc un champ d'application très large et englobe également beaucoup de données de recherche qui sont mises à disposition en tant qu'*ORD* sur Internet.

Le traitement de **données anonymisées et de données matérielles** (par exemple, des données concernant l'usure d'une turbine d'avion), qui n'ont, dès le départ, aucun lien avec une personne, n'en fait pas partie. L'anonymisation transforme les données personnelles de telle sorte que le lien avec une

⁵⁶ THOUVENIN, nbp. 20, 560 f. ; SHK UWG-Mabillard, nbp. 29, art. 6 N 1 et les références citées.

⁵⁷ OHLY ANSGAR, Harmonising the Protection of Trade Secrets: Challenges and Perspectives, in : Werra (Ed.), La protection des secrets d'affaires / The Protection of Trade Secrets, Zurich 2013, 32 ; MARCO BRONCKERS/NATHALIE M. MCNELIS, Is the EU obliged to improve the protection of trade secrets? An inquiry into TRIPS, the European Convention on Human Rights and the EU Charter of Fundamental Rights, EIPR 2012, 673 ss., 677.

⁵⁸ OHLY ANSGAR, Harmonising the Protection of Trade Secrets: Challenges and Perspectives, in : Werra (Ed.), La protection des secrets d'affaires / The Protection of Trade Secrets, Zurich 2013, 33 ; INGO MEITINGER, Die globale Rahmenordnung für den Schutz von Geschäftsgeheimnissen im TRIPS-Abkommen der WTO und ihre Auswirkungen auf die Rechtslage in der Schweiz, sic! 2002, 145 ss., 147.

personne déterminée ne peut plus être établi ou seulement au prix d'un effort disproportionné⁵⁹. La question de savoir quand les données personnelles peuvent être considérées comme anonymisées, n'est à ce jour pas suffisamment claire. Il n'est notamment pas clair à partir de quel degré d'abstraction une réidentification apparaît comme une tâche disproportionnée. En outre, la question de savoir dans quelle mesure une anonymisation est même possible d'un point de vue technique est controversée. Les développements dans le domaine de l'IA et du *Big Data* permettent justement de faire des déductions de plus en plus simples à partir d'un ensemble de données prétendument anonymisées afin d'identifier des personnes déterminées ou déterminables.

Les institutions du domaine des EPF, en tant qu'organes fédéraux, ne peuvent traiter des données personnelles que s'il existe pour cela une **base légale**. C'est le cas. Conformément à l'article 36c al. 1 de la Loi sur les EPF, les EPF et les établissements de recherche peuvent traiter des données personnelles, y compris des données sensibles, dans le cadre de projets de recherche, dans la mesure où cela est nécessaire pour le projet concerné. Lors du traitement des données personnelles, les institutions du domaine des EPF doivent assurer le respect des dispositions de la LPD. Cela est indiqué expressément à l'article 36c al. 2 de la Loi sur les EPF, mais cela ressort déjà de la LPD, parce que du point de vue du droit de la protection des données, les institutions du domaine des EPF sont à qualifier comme des organes fédéraux (article 2 al. 1 let. b lu en combinaison avec l'article 5 let. i LPD).

Conformément à l'article 39 LPD, les organes fédéraux sont en droit de traiter des données personnelles **à des fins ne se rapportant pas à des personnes**, notamment dans le cadre de la recherche, de la planification ou de la statistique, si les quatre conditions suivantes sont réunies : (i) les données sont rendues anonymes dès que la finalité du traitement le permet ; (ii) l'organe fédéral ne communique des données sensibles à des personnes privées que sous une forme ne permettant pas d'identifier les personnes concernées ; (iii) le ou la destinataire ne communique les données à des tiers qu'avec le consentement de l'organe fédéral qui les lui a transmises ; et (iv) les résultats du traitement ne sont publiés que sous une forme ne permettant pas d'identifier les personnes concernées. Ces dispositions s'appliquent également à la recherche au sein des institutions du domaine des EPF. L'article 36c al. 1 de la Loi sur les EPF n'est que la base légale, qui est nécessaire *afin que* les institutions puissent traiter des données personnelles dans le cadre de la recherche ; l'article 39 LPD contient des dispositions spécifiques sur la manière dont le traitement doit être effectué.

Les conditions de l'article 39 LPD visent certes la publication de résultats de la recherche dans des publications scientifiques, mais elles s'appliquent aussi à la **publication de données de recherche**. L'exigence de l'anonymisation est indiquée à deux reprises par l'article 39 LPD : lors du traitement de

⁵⁹ BEAT RUDIN, in : Baeriswyl/Pärli/Blonski (Ed.), Stämpfli Handkommentar, Datenschutzgesetz (DSG), Bern 2021, art. 5 N 13 ; GABOR P. BLECHTA/LUCA DAL MOLIN/KIRSTEN WESIAK-SCHMIDT, in : Blechta/Vasella (Ed.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz (DSG/BGÖ), Bâle 2024, art. 5 N 35.

données sous (i) et lors de la publication de résultats sous (iv). Il est donc clair que (i) les données personnelles doivent être anonymisées dès que possible lors de leur traitement pour la recherche et (ii) qu'elles ne peuvent être publiées que sous une forme anonymisée. **Par conséquent, les données personnelles ne doivent être mises à disposition que sous une forme anonymisée en tant qu'ORD.**

C. LIMITES POUR LES ORD

1. Problématique et Approche

Lors de la mise à disposition de données de recherche en tant qu'ORD, les dispositions du droit (objectif applicable doivent être respectées et il convient de vérifier si des tiers peuvent faire valoir des droits (subjectifs) (par exemple, droits d'auteur ou droits contractuels) qui s'opposent à la mise à disposition de données de recherche en tant qu'ORD.

Sous le titre « **Limites légales** », il est examiné si le droit fédéral contient des dispositions légales qui s'opposent à la mise à disposition de données de recherche en tant qu'ORD. Pour répondre à cette question formulée de façon très large, il convenait de déterminer lors d'une première étape les lois fédérales susceptibles de contenir des normes qui s'opposent à la mise à disposition de données de recherche par les institutions du domaine des EPF. La sélection des actes législatifs potentiellement pertinents a été définie par le domaine d'application des lois fédérales respectives et le domaine d'activité des institutions du domaine des EPF. La liste des actes législatifs potentiellement pertinents a été vérifiée lors de plusieurs réunions avec des représentants de toutes les institutions du domaine des EPF afin de déterminer leur pertinence et leurs lacunes. Ce faisant, aucun autre domaine d'application n'a été identifié qui devrait également être examiné.

Toutefois, au vu de la **problématique large**, on peut supposer que le droit fédéral contient d'autres dispositions qui s'opposent à la mise à disposition de données de recherche en tant qu'ORD qui n'ont pu être identifiées lors de notre démarche et qui n'ont donc pas été prises en compte dans ce rapport. Les chercheurs et/ou les services juridiques des institutions du domaine des EPF devront donc vérifier, **pour chaque ensemble de données concret, s'il existe des dispositions qui s'opposent à la mise à disposition de données**. En règle générale, il devrait être tout à fait possible d'apprécier cette question concrète parce que les chercheurs et/ou les services juridiques des institutions respectives connaîtront les normes pertinentes pour le domaine de recherche concerné.

Sur la base de la démarche esquissée, les domaines d'application suivants ont été identifiés et examinés : le droit du contrôle des exportations, le droit de la sécurité d'information, le droit de la santé, le droit du génie génétique, le droit de l'environnement, le droit des produits chimiques, le droit des denrées alimentaires, le droit de l'énergie et de l'énergie nucléaire, le droit de la protection animale ainsi que le droit des marchés financiers. Comme indiqué, il convient de supposer qu'il existe d'autres

domaines de réglementation contenant des dispositions qui s'opposent à la mise à disposition de données de recherche en tant qu'*ORD*. Par conséquent, les explications suivantes **ne doivent pas** être comprises **comme une présentation exhaustive de toutes les limites légales des *ORD***.

Sous le titre « **Droit des tiers** » sont examinés les droits (subjectifs) de tiers et les obligations contractuelles qui peuvent s'opposer à la publication et à la réutilisation de données de recherche en tant qu'*ORD*.

2. Limites légales

2.1. Contrôle des exportations

Des restrictions à l'exportation peuvent s'appliquer aux données de recherche. Selon la loi sur le contrôle des biens (LCB)⁶⁰, les biens ne sont pas que des marchandises physiques mais également des logiciels et des technologies, c'est-à-dire des informations, qui sont nécessaires au développement, à la fabrication ou à l'utilisation d'un bien mais qui ne sont pas accessibles au public et ne servent pas à la recherche scientifique fondamentale (article 3 let. d LCB).

Les institutions de recherche doivent respecter les dispositions⁶¹ de contrôle des exportations. L'exportation de données de recherche peut, dans certains cas, nécessiter une autorisation ou être complètement interdite. La question de savoir si de telles limites s'appliquent est déterminée selon le contenu des données de recherche et le pays de destination. Lorsque les données de recherche sont mises à disposition en tant qu'*ORD*, le contrôle des exportations est particulièrement ardu car le transfert ne peut être physiquement contrôlé aux frontières et, de façon générale, les données peuvent être mises à disposition dans le monde entier.

Si les données de recherche contiennent des informations sur la fabrication de biens sensibles, leur exportation sera toujours soumise à autorisation. Selon l'article 3, let. b LCB, les données sensibles ne sont pas seulement des données issues de la technologie des armements, mais incluent aussi de nombreuses données à première vue inoffensives, dans la mesure où elles peuvent également être utilisées à des fins militaires (biens à double usage). Les biens à double usage ou les paramètres pour leur qualification sont répertoriés à la liste des biens ayant une double finalité d'usage qui sont contenus

⁶⁰ Loi fédérale sur le contrôle des biens utilisables à des fins civiles et militaires, des biens militaires spécifiques et des biens stratégiques, RS 946.202.

⁶¹ En Suisse, de nombreux actes législatifs sont appliqués dans le cadre du contrôle des exportations, notamment la loi sur le contrôle des biens (LCB), l'Ordonnance sur le contrôle des biens, (OCB), Ordonnance sur l'exportation et le courtage de biens destinés à la surveillance d'Internet et des communications mobiles (OSIC), la Loi sur les embargos (Lemb), la Loi fédérale sur le matériel de guerre (LFMG) et les listes de biens applicables. En outre, il existe des conventions internationales : Traité sur le commerce des armes (Arms Trade Treaty [ATT]) ; l'Arrangement de Wassenaar (Wassenaar Arrangement [EWA]) ; Convention sur les armes chimiques (CAC).

dans les annexes 1 et 2 de l'Ordonnance sur le contrôle des biens (OCB)⁶². Il s'agit en principe de biens à double usage, fabriqués à l'origine pour un usage civil, mais qui, en raison de leurs caractéristiques, peuvent également être utilisés à des fins militaires. Exemples : informations dans le domaine des télécommunications, de l'électronique, de la chimie, de la technique navale ou de la technique de cryptage. Une caractéristique essentielle des biens à double usage – par opposition aux biens militaires spécifiques ou au matériel de guerre – est que leur domaine d'application ou leur utilisation finale n'est souvent pas claire. L'annexe 3 de l'OCB dresse la liste de ce qui est nécessaire pour une intervention militaire, par exemple des informations sur la production d'agents chimiques ou biologiques, l'équipement associé ou l'utilisation de substances radioactives.

La LCB s'applique à l'exportation de données de recherche qui ne sont pas encore accessibles au public. Elle ne s'applique pas à l'exportation de données de recherche qui sont déjà généralement connues et accessibles. Les sources d'information sont généralement accessibles lorsqu'elles sont techniquement adaptées et destinées à fournir des informations au public. Pour les données de recherche, cela signifie en particulier que les données déjà publiées ou connues de tous (par exemple, dans une publication scientifique) ne sont pas soumises à des restrictions en matière de contrôle des exportations et peuvent donc être publiées en tant qu'*ORD*.

Les restrictions en matière de contrôle des exportations ne s'appliquent pas aux informations issues de la recherche scientifique fondamentale. Selon l'annexe 1 de l'OCB, la recherche fondamentale consiste en « [...] des travaux expérimentaux ou théoriques visant principalement à obtenir de nouvelles connaissances sur les principes fondamentaux de phénomènes ou de faits, qui ne sont pas orientés en premier lieu vers un objectif ou un but pratique spécifique ».

La manière dont la technologie et les logiciels sont exportés n'a pas d'importance du point de vue de la LCB. Il suffit que les biens parviennent au client à l'étranger afin de mettre en œuvre les conséquences juridiques de la LCB. Les termes d'exportation et de transit recouvrent donc également la transmission non matérielle, par exemple, via des câbles de données. La question de savoir ce qu'il en est lorsque les données ne sont pas exportées mais mises à disposition pour téléchargement sur un serveur situé en Suisse, reste non élucidée. Du moins lorsque l'accès aux données de recherche se fait par le biais de centres de stockage et que les destinataires doivent s'enregistrer avant de télécharger les données, est-il possible de savoir vers quel pays de destination les données de recherche sont acheminées et d'empêcher l'exportation vers certains pays. Toutefois, un abus par contournement de l'enregistrement ne peut pas être exclu. D'un point de vue juridique, la question de savoir quels mécanismes de sécurité et de contrôle sont nécessaires à la mise à disposition de données de recherche en tant qu'*ORD* par le biais de centres de stockage n'a pas encore été examinée en détail et n'est pas claire.

⁶² Ordonnance sur le contrôle des biens utilisables à des fins civiles et militaires, des biens militaires spécifiques et des biens stratégiques, RS 946.202.1.

Par conséquent, il peut être retenu que les données de recherche destinées à être publiées en tant qu'*ORD* doivent être examinées selon les dispositions en matière de contrôle des exportations afin de déterminer si elles contiennent des informations ou des logiciels soumis à autorisation ou interdits.

L'examen doit être effectué au cas par cas pour les données concrètes. Les données de recherche contenant des informations interdites par la LCB ne peuvent pas être mises à disposition en tant qu'*ORD*. Afin que des données de recherche soumises à autorisation puissent être publiées en tant qu'*ORD*, une autorisation d'exportation doit être obtenue pour tous les pays, si l'on veut que l'accès aux *ORD* soit possible sans restriction depuis tous les pays.

Par conséquent, la publication de données de recherche en tant qu'*ORD* est exclue si ces données peuvent être qualifiées de biens à double usage. La qualification des données de recherche en tant que biens à double usage s'effectue sur la base de la liste des biens à double usage figurant aux annexes 1 et 2 de l'OCB.

2.2. Droit de la sécurité de l'information

Les données de recherche peuvent contenir des informations qui, du point de vue de l'État, sont à considérer comme sensibles. De telles informations peuvent être soumises à la loi sur la sécurité de l'information (LSI), ce qui limite leur utilisation en tant qu'*ORD*.

La LSI vise à garantir la sécurité du traitement des informations relevant de la compétence de la Confédération et la sécurité de ses moyens informatiques (article 1 al. 1 LSI). Elle vise ainsi à protéger différents intérêts publics, tels que la capacité de décision et d'action des autorités et la sécurité intérieure et extérieure de la Suisse (article 1 al. 2 LSI). La LSI oblige entre autres l'administration fédérale qui comprend en outre des unités administratives décentralisées à teneur des dispositions régissant leur organisation⁶³. Les institutions du domaine des EPF sont des unités administratives décentralisées et ainsi concernées par la LSI (cf. annexe 1 : liste des unités administratives de l'administration fédérale, B., VI., chiffre 2.2.5-2.2.10, Ordonnance sur l'organisation du gouvernement et de l'administration).

La LSI prévoit que le Conseil fédéral peut limiter l'application de la loi aux organisations de l'administration fédérale décentralisée qui exercent des activités sensibles en matière de sécurité ou qui utilisent ou accèdent aux moyens informatiques de la Confédération pour l'exercice de leurs tâches (art. 2, al. 3 LSI). Le Conseil fédéral a fait usage de cette possibilité dans l'ordonnance sur la sécurité de l'information (OSI) et a également précisé à l'article 2, paragraphe 2, de l'OSI quelles dispositions de la

⁶³ Ainsi le message relatif à Loi fédérale sur la sécurité de l'information du 22 février 2017, FF 2017 2953 ss., 3012. Voir aussi l'art. 2 al. 3 de la Loi sur l'organisation du gouvernement et de l'administration (LOGA), qui le dit expressément.



LSI s'appliquent à ces unités décentralisées de l'administration fédérale. Le Département fédéral de l'économie, de la formation et de la recherche (DEFR) a confirmé par courrier du 17 décembre 2024 qu'aucune des unités décentralisées du DEFR - et donc aucune institution du domaine des EPF - n'exerce en permanence des activités sensibles en matière de sécurité. Les institutions du domaine des EPF ne sont donc pas entièrement soumises à la LSI. Cependant, la LSI s'applique lorsque les institutions du domaine des EPF traitent des informations classifiées de la Confédération ou utilisent ou accèdent à des moyens informatiques de la Confédération (art. 2, al. 3, LSI en relation avec l'art. 2, al. 2, OSI).

Selon la LSI, les informations susceptibles de « nuire » aux intérêts publics, si elles sont portées à la connaissance d'une personne non autorisée, sont classifiées « internes » (article 13 al. 1 LSI). Les informations susceptibles de « nuire considérablement » aux intérêts publics, si elles sont portées à la connaissance d'une personne non autorisée, sont classifiées « confidentielles » (article 13 al. 2 LSI). Les informations susceptibles de « nuire gravement » aux intérêts publics, si elles sont portées à la connaissance d'une personne non autorisée, sont classifiées « secrètes » (article 13 al. 3 LSI). Si des informations ne remplissent pas les critères de l'article 13 de la LSI, elles ne sont pas classifiées et ne sont pas soumises à des dispositions juridiques particulières en Suisse, sauf s'il s'agit de données personnelles ou si des dispositions spécifiques s'appliquent (par exemple, pour les secrets de fonction). Toutefois, si elles sont classifiées, les informations correspondantes ne sont pas librement accessibles. Seules peuvent y accéder les personnes qui offrent toutes les garanties qu'elles les traiteront correctement et qui en ont besoin pour accomplir une tâche légale et, le cas échéant, disposent d'une autorisation d'accès qui leur a été conférée contractuellement (article 14 al. 1 let. a LSI). Cela peut rendre impossible une utilisation en tant qu'*ORD*.

Les exigences sont fixées pour le domaine des EPF et d'autres unités administratives décentralisées dans les dispositions d'exécution de l'Ordonnance sur la sécurité de l'information (OSI). Le principe est de limiter autant que possible la communication et la mise à disposition d'informations classifiées (article 16 al. 1 OSI). Les différentes unités administratives adoptent en outre régulièrement des directives (par exemple, les *Research Data Management Guidelines* des EPF) dans lesquelles elles déterminent leurs propres exigences et concrétisations en matière de sécurité de l'information, adaptées à leur domaine⁶⁴.

Comme par définition les informations classifiées ne peuvent être mises à disposition que d'un cercle restreint de personnes, il est exclu de rendre de telles informations accessibles en tant qu'*ORD*.

⁶⁴ À titre d'exemple, l'EPF Zurich l'a fait dans sa directive « Sécurité d'information à l'EPF Zurich » du 9 avril 2018.

2.3. Droit de la santé

2.3.1. Généralités

Les données du secteur de la santé sont fortement réglementées en Suisse. Les données sensibles, souvent liées à des personnes, sont la règle plutôt que l'exception dans ce secteur. Les personnes concernées sont particulièrement vulnérables, notamment lorsqu'on agit sur leur corps pour collecter des données, par exemple à l'occasion de prises de sang. En outre, il existe une asymétrie d'information difficile à résoudre entre les médecins ou les chercheurs et les patient(e)s.

Le personnel médical et ses assistants sont donc soumis au secret professionnel protégé par le droit pénal (article 321 code pénal ; CP) qui leur interdit de révéler un secret professionnel sans l'accord du/de la patient(e). La violation de secrets professionnels dans la recherche sur l'être humain est également punissable (article 321^{bis} CP). Le principe du droit de la santé appelé *informed consent* (consentement éclairé) revêt une grande importance. Comme le système de santé en Suisse relève principalement du ressort des cantons, les soins médicaux classiques sont en premier lieu soumis au droit cantonal (par exemple, les lois cantonales sur la santé). Il a donc été renoncé à inclure des explications complémentaires sur les questions juridiques liées aux soins médicaux.

2.3.2. Recherche dans le domaine humain

Dans de nombreux domaines, la recherche est largement tributaire de l'utilisation de données issues du secteur de la santé. Par conséquent, l'article 118b CF a conféré à la Confédération la compétence de légiférer sur la recherche sur l'être humain « dans la mesure où la protection de la dignité humaine et de la personnalité l'exige » (al. 1 phrase 1). Ce faisant, elle veille à sauvegarder la liberté de la recherche et à tenir compte de l'importance de la recherche pour la santé et la société (al. 1 phrase 2).

Sur cette base la Confédération a adopté la **Loi relative à la recherche sur l'être humain (LRH)**. Celle-ci s'applique à toute « la recherche sur les maladies humaines et sur la structure et le fonctionnement du corps humain », entre autres lorsque du matériel biologique et des données personnelles liées à la santé sont utilisés (article 2 al. 1 let. d et e LRH). Cette notion de recherche peut non seulement recouvrir toute la recherche médicale⁶⁵, mais également la recherche sur la prévention des accidents ou des blessures sportives ou la recherche en psychologie de la santé, ainsi que la recherche en sciences sociales et humaines portant sur le rapport entre les conditions sociales et des maladies spécifiques ou

⁶⁵ Celle-ci concerne selon BENEDIKT VAN SPYK, in : Rüttsche (Hrsg.), Stämpflis Handkommentar, Humanforschungsgesetz (HFG), Loi fédérale du 30 septembre 2011 relative à la recherche sur l'être humain, Bern 2015, Art. 3 N 16 par exemple les causes physiques et psychiques des maladies (recherche fondamentale); le transfert des connaissances fondamentales au domaine clinique (recherche translationnelle); l'origine, l'évolution, le diagnostic, la prophylaxie ainsi que le traitement des maladies (recherche clinique); la fréquence et la répartition des maladies dans la société (recherche épidémiologique).

les impacts sociétaux des maladies⁶⁶. La LRH est également applicable aux essais cliniques avec des produits thérapeutiques (article 53 Loi sur les produits thérapeutiques). L'applicabilité de la LRH est à examiner au cas par cas.

Dans le contexte des *ORD*, les dispositions spécifiques relatives aux données personnelles liées à la santé sont pertinentes. La LRH régit non seulement la collecte des données, par exemple à l'occasion de projets de recherche avec des personnes (sous forme de sondages ou d'observations), mais aussi l'utilisation secondaire, c'est-à-dire la **réutilisation** de telles données. La notion de réutilisation est comprise de manière très large. Toute opération effectuée à des fins de recherche avec du matériel biologique déjà prélevé ou des données déjà collectées est considérée comme une réutilisation de matériel biologique (article 24 Ordonnance relative à la recherche sur l'être humain [ORH])⁶⁷.

La LRH fait une distinction entre la réutilisation de matériel biologique et de données génétiques d'une part (article 32 LRH) et les données personnelles non génétiques liées à la santé d'autre part (article 33 LRH). Leur réutilisation est régie par des dispositions différentes selon la catégorie, brièvement décrites ci-après :

Conformément à l'article 32 al. 1 LRH le matériel biologique et les données génétiques peuvent être réutilisés pour *un* projet de recherche sous une forme *non codée* lorsque la personne concernée a donné son consentement éclairé. En revanche, lorsque le matériel et les données sont *codés* (pseudonymisés), c'est-à-dire la relation avec une personne déterminée se fait au moyen d'une clé (cf. article 3 let. h LRH), et ne sont ainsi déterminables que pour les personnes pouvant décoder les informations codées, la réutilisation *à des fins de recherche* n'est permise *de façon générale* que si la personne concernée a donné son consentement éclairé (article 32 al. 2 LRH ; soit « consentement général »). Si du matériel biologique et des données génétiques doivent être *anonymisés* et ensuite réutilisés de manière générale *à des fins de recherche*, la personne concernée doit être informée au préalable et ne doit pas s'être opposée à l'anonymisation (article 32 al. 3 LRH)⁶⁸.

Pour les données non génétiques liées à la santé, les possibilités de réutilisation sont plus larges. Elles peuvent être réutilisées *de manière générale* sous forme *non codée à des fins de recherche* si la personne concernée a donné son consentement éclairé (article 33 al. 1 LRH ; consentement général). Lorsque les données sont *codées*, la réutilisation *à des fins de recherche* est *généralement* autorisée,

⁶⁶ SHK HFG-VAN SPYK, nbp. 65, art. 3 N 19.

⁶⁷ L'Ordonnance mentionne explicitement le fait de se procurer, de regrouper ou de collecter, l'enregistrement ou le catalogage, la conservation ou la saisie dans des biobanques ou des banques de données ainsi que le fait de rendre accessibles, de mettre à disposition ou de communiquer du matériel biologique ou des données personnelles liées à la santé.

⁶⁸ Voir pour l'ensemble : SAMUEL MÄTZLER, Datenschutz in der (Human-)Forschung: Grundlagen und Probleme bei der Sekundärnutzung von Personendaten, in : Jusletter du 30 janvier 2023, para. 44.

pour autant que la personne concernée ait été informée au préalable et qu'elle ne s'y soit pas opposée. (article 33 al. 2 LRH)⁶⁹.

La réutilisation de données liées à la santé collectées de manière anonyme et anonymisées n'entre pas dans le champ d'application de la LRH et est donc autorisée sans condition⁷⁰. Cependant, cela ne concerne que la réutilisation de données déjà collectées.

Conformément à l'article 34 LRH, le matériel biologique et les données personnelles liées à la santé peuvent être réutilisés à titre exceptionnel à des fins de recherche si (1) l'obtention du consentement ou l'information sur le droit d'opposition est impossible ou pose des difficultés disproportionnées, ou on ne peut raisonnablement l'exiger de la personne concernée ; (2) aucun document n'atteste un refus de la personne concernée ; et (3) l'intérêt de la science prime celui de la personne concernée à décider de la réutilisation de son matériel biologique ou de ses données (article 34 let. a-c LRH).

Si le matériel ou les données sont utilisés dans le cadre d'un projet de recherche relevant de la LRH, celui-ci est toujours soumis à autorisation (article 45 al. 1 let. a LRH). Lorsqu'il s'agit d'une réutilisation sur la base de l'article 34 LRH, une autorisation demeure également nécessaire (article 45 al. 1 let. b LRH).

L'autorisation est délivrée par la commission d'éthique cantonale compétente, qui doit vérifier les exigences éthiques, juridiques et scientifiques de la LRH et contrôler en particulier si la protection des personnes concernées est assurée (article 51 al. 1 LRH). La commission d'éthique compétente est celle du canton dans lequel la recherche est réalisée (article 47 al. 1 LRH). Il n'existe pas de commission d'éthique fédérale pour le domaine de la recherche sur l'être humain ; les autorités fédérales doivent également rendre des comptes à une commission d'éthique cantonale.

En vertu de la LPD, les données qui relèvent de la LRH et qui présentent donc un lien avec des personnes ne peuvent pas être rendues accessibles en tant qu'*ORD*. En ce qui concerne la LRH, les dispositions spéciales relatives à la réutilisation encore plus restrictives doivent être respectées. La notion de réutilisation comprend également la conservation ou la saisie dans des biobanques ou des banques de données (article 24 let. c ORH) et le fait de rendre accessibles, de mettre à disposition ou de communiquer du matériel biologique ou des données personnelles liées à la santé (article 24 let. d ORH). Les articles 32-34 LRH doivent donc également être respectés pour de tels actes ; une autorisation de la commission d'éthique n'étant cependant pas nécessaire tant que la réutilisation n'a pas lieu dans le cadre d'un projet de recherche concret (par exemple, en cas de simple stockage dans une base de données).

⁶⁹ Voir pour l'ensemble : MÄTZLER, nbp. 68, para. 45.

⁷⁰ SHK HFG-RUDIN, nbp. 65 **Error! Bookmark not defined.**, art. 33 N 18.

Les données non liées à des personnes n'entrent pas dans le champ d'application de la LRH et peuvent donc en principe être mises à disposition en tant qu'*ORD*. Il convient de noter que, dans le cas de données génétiques (et de matériel biologique), il existe une **obligation d'information** préalable même pour le **processus d'anonymisation** et que l'anonymisation n'est autorisée que si la personne concernée n'a pas fait usage de son droit d'opposition.

2.3.3. Recherche dans le domaine non humain

La LRH ne s'applique ni à la recherche pratiquée sur du matériel biologique anonymisé (article 2 al. 2 let. b LRH) ni aux données liées à la santé qui ont été collectées anonymement ou qui ont été anonymisées (article 2 al. 2 let. c LRH). Les données correspondantes ne sont en principe pas réglementées en droit suisse. Toutefois, si des données personnelles sont traitées en dehors du champ d'application de la LRH, les dispositions générales en matière de protection des données s'appliquent au traitement des données personnelles⁷¹. Celles-ci autorisent le traitement à des fins ne se rapportant pas à des personnes, notamment pour la recherche, sous certaines conditions (article 31 al. 2 let. e LPD pour des personnes privées ; article 39 LPD pour des autorités fédérales), mais pas la mise à disposition de données non anonymisées en tant qu'*ORD*⁷².

Le *soft law* et les normes scientifiques jouent un rôle central tant pour les données personnelles que pour les données anonymisées. De nombreuses revues spécialisées et institutions de financement de la recherche exigent également pour des projets de recherche qui n'entrent pas dans le champ d'application de la LRH, la preuve de l'acceptabilité sur le plan éthique. Ainsi, dans la pratique, il existe aussi certaines dispositions à respecter pour ce type de données. Ces dispositions peuvent également s'étendre à l'utilisation d'*ORD*. Une vérification est généralement réalisée par les commissions d'éthique des institutions de recherche, telle que la commission éthique des EPF Zurich⁷³. Cette vérification n'a toutefois lieu que si aucune vérification (juridiquement contraignante) ne doit être effectuée par la commission d'éthique cantonale.

D'un point de vue juridique, seules les dispositions de la LPD s'appliquent : les données ne peuvent donc être mises à disposition en tant qu'*ORD* que sous forme anonymisée. Il est toutefois possible que les revues spécialisées et les institutions de financement de la recherche aient des exigences plus strictes.

⁷¹ cf. supra, 0.

⁷² cf. supra, 0.

⁷³ Voir <<https://ethz.ch/de/die-eth-zuerich/organisation/gremien-gruppen-kommissionen/ethikkommission.html>> (dernière visite le 27 mai 2024).

2.3.4. D'autres règles

Il existe d'autres dispositions dans des lois spéciales qui peuvent avoir un impact sur les *ORD*. Des règles spéciales existent par exemple pour l'analyse génétique humaine. L'article 10 de la Loi fédérale sur l'analyse génétique humaine (LAGH)⁷⁴ prévoit, par exemple, que des échantillons et des données génétiques sont à protéger de toute utilisation ou de tout traitement non autorisés au moyen de mesures techniques et organisationnelles appropriées. En revanche, la Loi sur la transplantation autorise la publication de données d'intérêt général qui concernent l'application de la loi (article 57 al. 3 de la Loi sur la transplantation). Toutefois, il est précisé que les personnes concernées ne doivent pas être identifiables. Les Ordonnances disposent ensuite que certaines données personnelles peuvent être communiquées à des tiers à des fins de recherche sous une forme anonymisée, à moins que la personne concernée n'ait consenti à cette communication ou qu'il existe une autorisation de la commission d'éthique compétente selon l'article 45 LRH (cf. L'article 34^m de l'Ordonnance sur l'attribution d'organes et article 49^h al. 2 de l'Ordonnance sur la transplantation ; aussi article 76 de l'Ordonnance sur la radioprotection). En revanche, dans le domaine des médicaments, les rapports sur les résultats des essais cliniques doivent également être obligatoirement anonymisés (article 73 al. 1 de l'Ordonnance sur les médicaments). Dans l'ensemble, au vu de ces exigences strictes, l'utilisation de telles données en tant qu'*ORD* est difficilement envisageable, d'autant plus qu'il est régulièrement fait référence aux exigences (également strictes) de la LRH.

Outre des restrictions, des dispositions légales spéciales peuvent également permettre l'utilisation de certaines données, par exemple en prévoyant un accès aux données. En application de la Loi sur l'enregistrement des maladies oncologiques (LEMO), des données peuvent être mises à disposition, par exemple, à des fins de recherche (article 23 al. 2 LEMO). En ce qui concerne la collecte et la réutilisation, la LEMO renvoie également à la LRH (article 23 al. 4 LEMO). Cela permet certes l'utilisation des données à des fins de recherche, mais pas la mise à disposition en tant qu'*ORD*.

Toutefois, certains actes législatifs prévoient également de manière explicite la mise à disposition en tant qu'*ORD*, par exemple sous la forme d'*Open Government Data* (OGD). L'article 21 al. 4 de la Loi fédérale sur l'assurance-maladie (LAMal) prévoit que l'office fédéral compétent met à disposition des fournisseurs de données, des milieux de la recherche et de la science ainsi que du public, les données nécessaires pour accomplir les tâches que la LAMal leur assigne. De la même manière, il est prévu, à l'occasion de la révision de la Loi sur les épidémies (LEp) de rendre utilisables les données collectées et générées dans le cadre de la LEp⁷⁵. Pour ce faire, il est prévu qu'elles soient mises à disposition du

⁷⁴ RS 810.12.

⁷⁵ DEPARTEMENT FEDERAL DE L'INTERIEUR (DFI), Révision partielle de la loi sur les épidémies, Rapport explicatif sur l'ouverture de la procédure de consultation du 29 novembre 2023, 33.

public et à des fins de recherche sous une forme anonymisée (article 59 al. 5 AP-LEp)⁷⁶. Conformément à la stratégie OGD de la Confédération, il faut s'attendre à ce que des réglementations similaires suivent dans d'autres domaines.

2.4. Génie génétique

Le droit sur le génie génétique régit l'utilisation d'animaux, de végétaux et d'autres organismes génétiquement modifiés ainsi que l'utilisation de produits issus de tels organismes (article 3 Loi sur le génie génétique (LGG)). La recherche, le développement, ainsi que la production, lorsqu'ils ont lieu en milieu confiné, sont régis par l'Ordonnance sur l'utilisation confinée (OUC)⁷⁷. Si les recherches et les essais aboutissent à la maturité d'un produit, différentes réglementations sectorielles s'appliquent en fonction du type de produit. S'il s'agit d'organismes qui, en tant que produits, sont destinés à être disséminés dans l'environnement, les règles de l'Ordonnance sur la dissémination dans l'environnement s'appliquent (ODE, par exemple pour les semences)⁷⁸. Les médicaments et les denrées alimentaires sont soumis à la législation sur les produits⁷⁹.

Le domaine du génie génétique comporte de nombreuses réglementations. Toutefois, la réglementation ne concerne que l'utilisation d'organismes génétiquement modifiés, c'est-à-dire les « entités biologiques, cellulaires ou non » (article 5 al. 1 LGG), et pas le traitement de données y afférentes. A priori, il n'existe pas de limites légales qui s'opposent à la publication de données de génie génétique en tant qu'*ORD*.

2.5. Droit de l'environnement

Le droit de l'environnement comprend, outre la Loi sur la protection de l'environnement (LPE)⁸⁰ et les ordonnances y afférentes, une série d'autres actes législatifs, notamment dans les domaines des déchets, des sites contaminés, de la biodiversité, de la biotechnologie, des sols, de l'électrosmog, du climat, du paysage, du bruit, de l'air, des dangers naturels, des forêts et bois ainsi que de l'eau⁸¹.

⁷⁶ EDI, nbp. 75, 33. La procédure de consultation pour l'avant-projet est terminée, cf. état actuel : <https://www.fedlex.admin.ch/de/consultation-procedures/ended/2023#https://fedlex.data.admin.ch/eli/dl/proj_/2023/5/cons_1> (consulté la dernière fois le 27 mai 2024).

⁷⁷ Ordonnance sur l'utilisation des organismes en milieu confiné, RS 814.912.

⁷⁸ Ordonnance sur l'utilisation des organismes en milieu confiné, RS 814.911.

⁷⁹ Médicaments : Loi fédérale sur les médicaments et les dispositifs médicaux (Loi sur les produits thérapeutiques, LPT), RS 812.21 ; Denrées alimentaires : Loi fédérale sur les denrées alimentaires et les objets usuels (Loi sur les denrées alimentaires, LDAI), RS 817.0.

⁸⁰ RS 814.01.

⁸¹ <<https://www.bafu.admin.ch/bafu/de/home/themen/recht/geltendes-umweltrecht.html>> (dernière visite le 27 mai 2024).

En raison du grand nombre de personnes directement concernées, le **principe de publicité** est largement appliqué dans le droit de l'environnement⁸². Les réglementations prévoient même parfois que les données doivent être rendues accessibles au public. Conformément à l'article 10d al. 1 LPE chacun peut consulter le rapport et les résultats de l'étude d'impact pour autant qu'aucun intérêt public ou privé prépondérant n'exige de les garder secrets. Le secret de fabrication et d'affaires reste, selon l'article 10d al. 2 LPE, protégé dans tous les cas. Cette obligation incombe toutefois à l'autorité qui publie l'information. Une fois que l'étude d'impact a été publiée, la LPE ne prévoit aucune restriction quant à la mise à disposition ultérieure des résultats, par exemple en tant qu'*ORD*.

Conformément à l'article 10e al. 1 LPE les autorités renseignent le public de manière objective sur la protection de l'environnement et sur l'état des nuisances qui y portent atteinte. Par « informations sur l'environnement », on entend les informations relatives au domaine d'application de la LPE et de la législation (fédérale ou cantonale) sur la protection de la nature et du paysage, la protection des sites naturels, la protection des eaux, la protection contre les dangers naturels, la sauvegarde des forêts, la chasse, la pêche, le génie génétique et la protection du climat (article 7 al. 8 LPE). Les informations sur l'environnement doivent être publiées si possible sous forme de données numériques ouvertes (article 10e al. 4 LPE).

Conformément à l'article 10 de la Loi sur la géoinformation (LGéo)⁸³, les **géodonnées de base** sont en principe accessibles au public et peuvent être utilisées par chacun à moins que des intérêts publics ou privés prépondérants ne s'y opposent. Les détails figurent dans l'Ordonnance sur la géoinformation (OGéo)⁸⁴. Celle-ci prévoit également certaines restrictions à la publication de géodonnées de base auxquelles elle attribue trois niveaux d'autorisation d'accès de A - C. Les niveaux d'autorisation d'accès aux géodonnées de base sont indiqués dans l'annexe 1 OGéo. En principe, l'accès aux géodonnées de base de niveau A est garanti. Toutefois, exceptionnellement, l'accès peut être limité, différé ou refusé (article 22 al. 2 OGéo), par exemple si la publication risque de compromettre la sûreté intérieure. Aucun accès n'est en principe garanti aux géodonnées de base de niveau B (article 23 al. 1 OGéo). Ce principe connaît des exceptions, si aucun intérêt lié au maintien du secret ne s'oppose à l'accès ou si les intérêts liés au maintien du secret peuvent être sauvegardés par des mesures juridiques, organisationnelles ou techniques (article 23 al. 2 OGéo). Aucun accès n'est garanti aux géodonnées de base de niveau C ; aucune exception n'est prévue (article 24 OGéo). Conformément à l'article 25 OGéo, l'autorisation d'utilisation de géodonnées de base à usage privé ou à des fins commerciales peut être délivrée. L'autorisation pour un usage privé n'autorise toutefois pas

⁸² THOMAS JUTZI, Unternehmenspublizität, Bern 2017, 48 ; ROLF H. WEBER, Datenschutz v. Öffentlichkeitsprinzip: Erläuterungen zu den Spannungsfeldern am Beispiel des Zürcher Informations- und Datenschutzgesetzes, Zurich 2010, N 173.

⁸³ Loi fédérale sur la géoinformation, RS 510.62.

⁸⁴ Ordonnance sur la géoinformation, RS 510.620.

les titulaires à rendre accessibles les géodonnées de base en tant qu'*ORD*, d'autant plus que l'autorisation d'utilisation n'est délivrée que pour l'usage privé par une personne déterminée et uniquement contre paiement d'une redevance. Comme l'accès aux géodonnées de base de niveau A est de toute façon accordé (article 22 al. 1 OGéo), il est probable qu'on puisse aussi les rendre accessibles en tant qu'*ORD*, sauf exception au sens de l'article 22 al. 2 OGéo.

En conclusion, il convient de noter que les données de recherche contenant des informations environnementales peuvent en principe être publiées en tant qu'*ORD*, sauf restriction exceptionnelle.

2.6. Droit de produits chimiques

La Loi sur les produits chimiques (LChimG)⁸⁵, l'Ordonnance sur les produits chimiques (OChi)⁸⁶, l'Ordonnance sur les produits biocides (OPBio)⁸⁷ et l'Ordonnance sur les produits phytosanitaires (OPPh)⁸⁸ ne contiennent pas de règles qui s'opposent à la publication de données de recherche dans ce domaine en tant qu'*ORD*.

Toutefois, l'Ordonnance sur les produits phytosanitaires (OPPh) prévoit que les rapports d'essais et d'études bénéficient de la protection des rapports (article 46 PSMV). Cette protection ne s'oppose pas en soi à une mise à disposition en tant qu'*ORD*. Toutefois, en principe, le service d'homologation ne peut pas utiliser les rapports protégés dans l'intérêt d'autres demandeurs d'autorisations de produits phytosanitaires, de phytoprotecteurs ou de synergistes et d'adjuvants (article 46 al. 3 OPPh). La période de protection des rapports est de dix ans (article 46 al. 4 OPPh).

L'OFSP peut également mettre à disposition de tiers des données issues de la banque de données sur le radon à des fins de recherche. Cela est toutefois soumis, entre autres, à la condition que les données ne soient pas transmises à des tiers (article 162 al. 5 let. b Ordonnance sur la radioprotection). Les données correspondantes ne peuvent donc pas être rendues accessibles en tant qu'*ORD*.

2.7. Droit des denrées alimentaires

Les bases légales pour les données du domaine des denrées alimentaires sont en premier lieu la Loi sur les denrées alimentaires (LDAI)⁸⁹ et l'Ordonnance sur l'exécution de la législation sur les denrées alimentaires (OELDAI)⁹⁰. L'article 40 al. 1 LDAI prévoit que la Confédération recueille et étudie les données scientifiques qu'exige l'application de la LDAI. Elle peut effectuer des études elle-même ou

⁸⁵ Loi fédérale sur la protection contre les substances et les préparations dangereuses, RS 813.1.

⁸⁶ Ordonnance sur la protection contre les substances et les préparations dangereuses, RS 813.11.

⁸⁷ Ordonnance concernant la mise sur le marché et l'utilisation des produits biocides, RS 813.12.

⁸⁸ Ordonnance sur la mise en circulation des produits phytosanitaires, RS 916.161.

⁸⁹ Loi fédérale sur les denrées alimentaires et les objets usuels, RS 817.0.

⁹⁰ RS 817.042.

avec la collaboration des cantons (article 40 al. 2 LDAI). Si cela est le cas, les résultats des études et de la recherche ne doivent pas être rendus accessibles au public, lorsque ceux-ci permettent d'identifier les fabricants, les distributeurs ou les produits concernés (article 24 al. 4 let. b LDAI). Il est possible que des institutions du domaine des EPF mènent des recherches sur la base de l'article 40 LDAI, ce qui pourrait s'opposer à la publication de données de recherche issues du domaine alimentaire en tant qu'*ORD*. En outre, les fondements juridiques ne contiennent aucune (autre) limite s'opposant à une mise à disposition de données de recherche en tant qu'*ORD*.

2.8. Droit de l'énergie et de l'énergie nucléaire

Le droit de l'énergie impose des limites à la publication de données de recherche pour la protection des infrastructures critiques. Les infrastructures critiques sont des processus, des systèmes et des institutions qui sont essentiels au fonctionnement de l'économie ou au bien-être de la population. Pour la Suisse, l'éventail des infrastructures critiques dans le droit de l'énergie comprend l'approvisionnement en gaz naturel, l'approvisionnement en pétrole, l'approvisionnement en électricité, l'approvisionnement en eau, le chauffage à distance et industriel, les déchets et les eaux usées⁹¹. L'inventaire des infrastructures critiques (inventaire PIC) définit les bâtiments et les installations qui revêtent une importance stratégique, soit au niveau national, soit au niveau cantonal. Il est classé confidentiel dans son intégralité. Les extraits qui ne contiennent qu'une partie des informations (par exemple, d'un canton ou d'un secteur) sont généralement classés comme confidentiels⁹². Si les données de recherche concernent des informations sur des infrastructures critiques, elles ne peuvent pas être rendues publiques en tant qu'*ORD*.

Dans le domaine de **l'énergie nucléaire**, il existe un intérêt public au maintien du secret à plusieurs égards, par exemple en ce qui concerne l'utilisation d'éléments radioactifs et l'exploitation de centrales nucléaires, afin de garantir la sécurité et la protection contre les actes de sabotage ou les attaques terroristes. L'article 91 al. 1 let. b de la Loi sur l'énergie nucléaire (LENu)⁹³ punit la révélation d'un secret. Est puni celui qui révèle ou rend accessible à des personnes non autorisées des faits ou des dispositifs tenus secrets et destinés à protéger les installations nucléaires, les matières nucléaires et les déchets radioactifs contre les atteintes de tiers et contre les conséquences de la guerre.

Il n'est pas possible de déterminer de façon abstraite quelles informations sont couvertes par la disposition pénale en cas de violation du secret de l'article 91 al. 1 let. b LENu. Lors de l'utilisation de données de recherche en rapport avec l'énergie nucléaire, il faut donc veiller à ce que celles-ci ne soient

⁹¹ OFFICE FEDERAL DE LA PROTECTION DE LA POPULATION, Stratégie nationale de protection des infrastructures critiques, Approche globale pour garantir l'approvisionnement en biens et prestations essentiels du 16 juin 2023, FF 2023 1659, 7 ss.

⁹² <<https://www.babs.admin.ch/de/die-kritischen-infrastrukturen>> (dernière visite le 27 mai 2024).

⁹³ RS 732.1.

rendues accessibles en tant qu'*ORD* que si elles peuvent être rendues accessibles au public conformément à l'article 74 al. 1 LENu et qu'il ne s'agit pas de faits ou de dispositifs tenus secrets et destinés à protéger les installations nucléaires, les matières nucléaires et les déchets radioactifs contre les atteintes de tiers et contre les conséquences de la guerre. Quiconque rend de telles données de recherche accessibles en tant qu'*ORD* est puni en vertu de l'article 91 al. 1 let. b LENu.

L'article 13 de l'Ordonnance sur l'énergie nucléaire (OENu)⁹⁴ comporte un autre obstacle pour les *ORD* en rapport avec les données issues de l'énergie nucléaire. L'article 13 OENu prévoit une obligation d'autorisation afin d'exporter et de faire le courtage de technologies concernant des matières nucléaires. Dans ce contexte, on entend par « technologies » les connaissances spécifiques, généralement non accessibles au public ou ne servant pas à la recherche scientifique fondamentale, sous la forme de données techniques ou d'une assistance technique, qui sont nécessaires au développement, à la production ou à l'utilisation de matières nucléaires. Si des données de recherche contenant de telles informations doivent être rendues accessibles en tant qu'*ORD*, une autorisation est requise. L'autorisation d'exportation et de courtage est délivrée si les exigences d'autorisation de l'article 7 let. a ss. OENu sont respectées. En particulier, la protection de l'être humain et de l'environnement, et la sûreté et la sécurité nucléaires doivent être garanties et aucun motif de non-prolifération des armes nucléaires soutenu par la Suisse ne doit s'y opposer. Il convient d'examiner au cas par cas quand les technologies relatives aux matières nucléaires respectent les autorisations d'exportation et de courtage. Sans une telle autorisation d'exportation et de courtage, ces données de recherche ne peuvent pas être rendues accessibles en tant qu'*ORD*.

Le droit de l'énergie et de l'énergie nucléaire comporte des limites juridiques qui s'opposent à la publication de certaines données de recherche en tant qu'*ORD*. Dans le droit de l'énergie, les limites concernent les données relatives à l'inventaire des infrastructures critiques qui doivent être traitées de manière secrète ou confidentielle. Dans le domaine de l'énergie nucléaire, il existe des restrictions pour les informations destinées à protéger les installations nucléaires, les matières nucléaires et les déchets radioactifs contre les atteintes de tiers et contre les conséquences de la guerre et pour les données dont l'exportation ou le courtage créerait un danger pour la sécurité nucléaire.

2.9. Droit de la protection animale

En droit de la protection animale il convient de respecter en premier lieu la Loi fédérale sur la protection des animaux (LPA)⁹⁵ et l'Ordonnance sur la protection des animaux (OPAn)⁹⁶, qui régissent la protection des vertébrés (donc des mammifères, des poissons, des oiseaux, des amphibiens et reptiles). Les

⁹⁴ RS 732.11.

⁹⁵ RS 45.

⁹⁶ RS 455.1.

invertébrés (par exemple des escargots, araignées, vers, etc.) sont exclus du champ d'application. Outre le droit de la protection et du bien-être des animaux, toute une série d'autres domaines juridiques concerne les animaux, par exemple dans l'élevage, le droit vétérinaire, les paiements directs agricoles, la protection des espèces, le droit de la chasse et de la pêche ou le droit des denrées alimentaires.

L'analyse des bases légales applicables dans le droit de la protection animale montre qu'il n'y a pas de limites légales qui s'opposeraient à la publication de données de recherche en tant qu'*ORD*.

2.10. Droit des marchés financiers

Dans le domaine du droit des marchés financiers, il faut notamment veiller au respect du secret bancaire. L'obligation de secret en application de l'article 47 de la Loi sur les banques (LB)⁹⁷ comprend toutes les connaissances issues de la relation commerciale entre la banque et le client, notamment des contrats bancaires, mais aussi des demandes et des offres pour d'autres opérations bancaires et les relations d'affaires entre banques⁹⁸.

L'obligation de confidentialité s'applique à toutes les personnes travaillant au sein d'une banque ou sur la base d'un contrat pour celle-ci. Une banque ne peut accorder l'accès aux données de ses clients à des personnes travaillant dans le domaine scientifique que s'il existe avec elles une relation de travail ou de mandat (article 47 al. 1 LB). L'anonymisation des données des clients dans une éventuelle publication reste dans tous les cas obligatoire à moins que les clients ne donnent explicitement leur accord à la divulgation⁹⁹. Les données bancaires anonymisées ne sont plus des données personnelles si, selon le cours normal des choses, aucune personne concernée ne peut mettre en œuvre les moyens qui peuvent raisonnablement être utilisés pour la réidentification. Les données bancaires échappent à la protection du secret bancaire lorsqu'elles sont anonymisées¹⁰⁰. Si des données bancaires ont été transmises à des chercheurs sous forme anonymisée, on peut généralement partir du principe que la publication de ces données en tant qu'*ORD* ne viole pas le secret bancaire et est donc licite. Les données soumises au secret bancaire ne peuvent donc être rendues accessibles que sous forme anonyme en tant qu'*ORD*.

⁹⁷ Loi fédérale sur les banques et les caisses d'épargne, RS 952.0.

⁹⁸ BEAT KLEINER/RENATE SCHWOB/CHRISTOPH WINZELER, Kommentar zum Bundesgesetz über die Banken und Sparkassen vom 8. November 1934 sowie zu der Verordnung vom 17. Mai 1972 (V) und der Vollziehungsverordnung (VV) vom 30. August 1961 (VV) – mit Hinweisen auf das Bankenrecht der Europäischen Union, auf das Allgemeine Dienstleistungsabkommen (GATS) und mit Erläuterungen zu den Maßnahmen gegen die Geldwäscherei, Zöbl/Schwob/Winzler/Kaufmann/Weber/Kramer (Ed.), Zurich 2015, art. 47 N 8 ss.

⁹⁹ BankG-Komm., KLEINER/SCHWOB/WINZELER, nbp. 98, art. 47 N 335, 360.

¹⁰⁰ CELIAN HIRSCH/EMILIE JACOT-GUILLARMOD, Les données bancaires pseudonymisées – Du secret bancaire à la protection des données, SZW 2020, 151 ss., 156.

En conclusion, il convient de retenir que les données de recherche soumises au secret bancaire ne peuvent pas être rendues accessibles en tant qu'*ORD*. Si les données bancaires des clients sont anonymisées, une publication en tant qu'*ORD* peut avoir lieu.

Les règles relatives aux services financiers¹⁰¹ et aux établissements financiers¹⁰² ne contiennent pas de limites juridiques pour les *ORD*.

3. Droit des tiers

La mise à disposition de données de recherche peut être entravée non seulement par des dispositions légales, mais aussi par les droits des tiers. Au premier plan, il y a les droits d'auteur, les droits découlant de la protection pénale du secret (article 162 CP), les droits issus de la LCD (article 5 let. c et article 6 LCD) et les droits issus du droit de la protection des données. En revanche, les brevets ne peuvent pas être opposés à la mise à disposition de données de recherche.

3.1. Droits d'auteur

Nous considérons qu'en règle générale ni les œuvres littéraires et artistiques ou prestations protégées ni les programmes d'ordinateur ne sont rendus accessibles en tout ou en partie en tant qu'*ORD*. Avant la mise à disposition d'*ORD*, il faut toujours **vérifier si les données contiennent des œuvres ou des parties d'œuvres protégées par le droit d'auteur**¹⁰³. C'est par exemple le cas lorsque des séquences suffisamment longues de code source ou de textes, d'images ou de photographies sont mises à disposition. Dans ce cas, il faut demander aux titulaires de droits d'auteur sur ces œuvres s'ils sont d'accord pour que leurs œuvres soient mises à disposition.

De grandes quantités de données de recherche, mises à disposition en tant qu'*ORD*, devront régulièrement être qualifiées de bases de données au sens du droit d'auteur. S'il s'agit **de bases de données structurées**, elles peuvent être protégées par le droit d'auteur. Avant la mise à disposition de données en tant qu'*ORD*, il faut donc toujours vérifier si les données peuvent être qualifiées de base de données, qui pourrait être protégée par le droit d'auteur. Si tel est le cas, il convient de demander aux titulaires des droits s'ils sont d'accord avec la mise à disposition de la base de données.

Les droits d'auteur appartiennent aux personnes qui ont créé la base de données (article 6 LDA). Dans la mesure où il s'agit de bases de données créées par des employés d'une institution du domaine des EPF, les droits d'auteur sur les bases de données appartiennent à ces employés (article 36 al. 1 de la Loi sur les EPF). Cette règle semble certes dénuée d'un peu de sens, d'autant plus que les droits

¹⁰¹ Loi fédérale sur les services financiers (LSFin), RS 950.1.

¹⁰² Loi fédérale sur les établissements financiers (LEFin), RS 954.1.

¹⁰³ cf. supra, B.1.2.

d'auteur sur le code source sont transférés de plein droit aux institutions du domaine des EPF (article 36 al. 2 de la Loi sur les EPF), mais elle résulte de façon non équivoque des dispositions de l'article 36 al. 1 et al. 2 de la Loi sur les EPF. Les employés peuvent ainsi décider eux-mêmes s'ils veulent rendre accessibles des bases de données en tant qu'*ORD*, dans la mesure où l'institution concernée du domaine des EPF n'a pas adopté de règlement interne qui prescrit un transfert des droits d'auteur sur les bases de données à l'institution ou une mise à disposition de données de recherche (et/ou de bases de données) en tant qu'*ORD*. Si une **base de données a été créée par des tiers, ils doivent être consultés**. Il faut toujours vérifier si les auteurs de la base de données ont cédé leurs droits à d'autres tiers, par exemple à une université, une maison d'édition ou un fournisseur commercial. Si tel est le cas, il faut obtenir leur accord.

3.2. Brevets

Les brevets sont délivrés pour des **inventions**, c'est-à-dire pour des **enseignements en vue d'une activité technique**¹⁰⁴. Ils confèrent à son titulaire le droit d'interdire à des tiers d'utiliser l'invention à titre professionnel (article 8 al. 1 LBI). L'utilisation comprend notamment la fabrication, l'entreposage, l'offre et la mise en circulation ainsi que l'importation, l'exportation, le transit et la possession à ces fins (article 8 al. 2 LBI). En ce qui concerne l'utilisation, il convient de distinguer les **brevets de produit et les brevets de procédé**. Par « utilisation », on entend, dans le cas des brevets de produit, la fabrication et la commercialisation de l'invention brevetée. Sont ainsi visés tous les actes (mais seulement ceux-là) concernant le produit protégé par le brevet, qui comprennent, outre la fabrication, l'entreposage, l'offre, la mise en circulation, etc., d'un tel produit. Pour les brevets de procédé, il y a utilisation lorsque le procédé est mis en œuvre, c'est-à-dire lorsque les étapes de procédé prévues dans les revendications du brevet sont réalisées.

Les données de recherche mises à disposition en tant qu'*ORD* peuvent contenir des inventions brevetées. Cela devrait être rarement le cas, mais ne peut être exclu. Cependant, la mise à disposition d'une invention sur Internet ne constitue **pas une utilisation d'une invention** au sens du droit des brevets, car elle ne permet pas de fabriquer un produit ou de mettre en œuvre un procédé. La mise à disposition ne peut donc pas être interdite par le titulaire du brevet.

Il convient également de noter que les brevets ne sont délivrés que si **l'invention est divulguée dans la demande de brevet**. Cela signifie que l'invention doit être exposée, dans la demande de brevet, de façon suffisamment claire et complète pour qu'un homme de métier puisse l'exécuter sur la base du

¹⁰⁴ MARK SCHWEIZER/HERBERT ZECH, in : Schweizer/Zech (Ed.), Stämpfli Handkommentar, Patentgesetz (PatG), Bundesgesetz über die Erfindungspatente vom 25. Juni 1954, Bern 2019, Art. 1 N 10; BGer 4A.12/1995 vom 31. Juli 1996, E. 4, in: sic! 1997, 77 ss. : Dans sa décision, le Tribunal fédéral a qualifié une invention technique « d'enseignement pour utiliser méthodiquement des forces naturelles contrôlables pour atteindre directement un résultat causal et perceptible ».

fascicule du brevet et en tenant compte des connaissances générales dans le domaine concerné (article 50 al. 1 LBI)¹⁰⁵. Comme le fascicule de brevet est publié sur le site Internet de l'Office des brevets lors de la délivrance du brevet, l'invention est en tout état de cause accessible au public dès la délivrance du brevet. Si les données de recherche rendues accessibles en tant qu'*ORD* devaient contenir une invention brevetée, elles ne divulgueraient pas d'informations qui ne soient pas déjà accessibles au public.

3.3. Droits découlant de la protection du secret par le droit pénal

Si des données de recherche en tant qu'*ORD* sont rendues accessibles alors que les chercheurs et/ou l'institution des domaines des EPF sont légalement ou contractuellement tenus au secret, il y a violation de l'article 162 CP. La personne physique qui a rendu les données accessibles peut être, sur plainte du détenteur du secret, punie d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire (article 162 CP).

C'est le **détenteur du secret** qui a le droit de porter plainte. Le détenteur du secret sera généralement une autre institution de recherche ou une entreprise qui a mis à disposition d'un chercheur ou d'une institution du domaine des EPF des données de recherche et qui a obligé les chercheurs ou l'institution à respecter le secret. Le détenteur du secret peut non seulement porter plainte, mais aussi demander la cessation de l'infraction et l'octroi de dommages-intérêts. Le droit à réparation découle du droit commun de la responsabilité délictuelle (article 41 CO lu en combinaison avec l'article 162 CP). Le droit de demander la cessation n'a pas été prévu de façon explicite, mais il peut être déduit du droit commun de la responsabilité délictuelle (article 41 ss. CO). En effet, celui-ci ne donne pas seulement droit à demander l'octroi de dommages-intérêts, mais aussi, à juste titre, la cessation de l'infraction¹⁰⁶.

3.4. Droits découlant de la LCD

La LCD s'applique à toutes les actions visant à influencer la concurrence sur un marché (donné). Il s'agit de toutes les actions qui sont **pertinentes pour le marché**, qui sont **orientées vers le marché ou la concurrence** et qui peuvent avoir un effet sur les relations entre concurrents ou sur les relations entre fournisseurs et acheteurs. En revanche, la LCD ne s'applique pas à la recherche scientifique et à la publication de ses résultats, tant que ces activités se déroulent dans un cadre académique¹⁰⁷. La LCD

¹⁰⁵ HGer SG, sic! 2009, 875 ss., 879 ss. – « Dichtmasse » ; SHK PatG-SUTTER/HOCHREUTENER, nbp. 104, art. 50 N 3 ss.

¹⁰⁶ MARTIN A. KESSLER, in : Widmer Lüchinger/Oser (Ed.), Basler Kommentar, Obligationenrecht I, art. 1-529 CO, Bâle 2020, art. 43 N 4 ; dans ce sens aussi MARTIN ECKERT, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 2016, 245 ss., 272 et URS HESS-ODONI, Die Herrschaftsrechte an Daten, in : Jusletter du 17 mai 2004, Rz. 39.

¹⁰⁷ BGer 6B_188/2013 du 4 juillet 2013, E. 6.3, et les références citées.

s'applique toutefois aux coopérations avec des entreprises privées et lorsque les résultats de la recherche (par exemple d'une start-up) doivent être exploités sur le marché.

La reprise et la mise à disposition de données de recherche en tant qu'ORD peut enfreindre **l'interdiction de la reprise directe (article 5 let. c LCD)** ou être qualifiée de **violation de secrets de fabrication et d'affaires (article 6 LCD)**. Toutefois, ce dernier cas ne se présente que si le contrevenant a surpris ou a eu indûment connaissance d'une autre manière des données¹⁰⁸.

Celui qui, par une violation d'une disposition de la LCD, subit une atteinte dans sa clientèle, son crédit ou sa réputation professionnelle, ses affaires ou ses intérêts économiques en général ou celui qui en est menacé, peut demander la cessation de l'infraction, la suppression des conséquences de la violation et des dommages-intérêts ainsi que la remise du gain (article 9 LCD). Une violation de l'article 5 let. c ou de l'article 6 LCD est en outre punissable ; l'auteur est puni, sur plainte, d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire (article 23 LCD). Le *data owner*, c'est-à-dire le **détenteur du contrôle effectif de données**, juridiquement protégé par les articles 5 let. c et 6 LCD, est en droit d'intenter une action en cessation, en suppression et en dommages-intérêts ou en remise du gain et à déposer plainte.

3.5. Droits issus de la protection des données

Le droit de la protection des données ne confère pas aux personnes concernées **un droit de contrôle global** sur les données les concernant, mais certains droits leur permettant de contrôler et de limiter dans une certaine mesure l'utilisation des données. Ces possibilités vont beaucoup plus loin lorsque les données sont traitées par une personne privée, en particulier par une entreprise. Le traitement par les entreprises repose dans certains cas sur le consentement des personnes concernées, qui peut être révoqué à tout moment¹⁰⁹. En outre, les personnes concernées peuvent s'opposer au traitement des données les concernant (article 30 al. 2 let. b LPD). Les deux constellations font que la personne privée peut seulement traiter les données si elle a un intérêt prépondérant au traitement des données (article 31 LPD).

Le traitement de données personnelles par des organes fédéraux repose toujours sur une **base légale**. Le consentement des personnes concernées n'est pas nécessaire pour ce traitement. Cela vaut également pour le traitement des données personnelles dans le cadre de la recherche par les institutions du domaine des EPF. Le fait que les personnes concernées donnent régulièrement leur consentement au traitement de données personnelles pour la recherche ne change rien à cette situation juridique. D'un point de vue éthique (en matière de recherche), on ne peut que se réjouir du fait que

¹⁰⁸ cf. supra, B.1.5.

¹⁰⁹ BSK DSG-BÜHLMANN/REINLE, nbp. 59, art. 6 N 316 ; SHK DSG-BAERISWYL, nbp. 59, art. 6 N 84.



l'obtention du consentement soit recherchée, qu'elle soit prévue dans de nombreuses normes et qu'elle constitue une pratique établie dans de nombreux domaines, mais cela **n'est pas exigé par le droit de la protection des données**. Ni pour le traitement dans le cadre d'un projet de recherche, ni pour la mise à disposition des données de recherche en tant qu'**ORD** sous forme anonymisée. Le traitement de données personnelles pour la recherche au sein des institutions du domaine des EPF ne reposant pas juridiquement sur un consentement, les personnes concernées ne peuvent pas davantage empêcher valablement le traitement des données les concernant en révoquant leur consentement ou en exerçant un droit d'opposition ou en demandant l'effacement. Les personnes concernées ne disposent donc pas de droits leur permettant d'empêcher la mise à disposition de « données personnelles » les concernant en tant qu'**ORD**.

Comme indiqué plus haut, les données personnelles ne peuvent être **rendues accessibles que sous forme anonymisée en tant qu'ORD**, en vertu des dispositions générales du droit de la protection des données¹¹⁰. Si cette condition est remplie, la LPD ne s'applique nullement à la mise à disposition des données. Pour cette raison, les personnes concernées ne disposent pas de droits en matière de protection des données qu'elles pourraient faire valoir contre la mise à disposition de données de recherche en tant qu'**ORD**.

4. Restrictions contractuelles

Les projets de recherche sont souvent réalisés dans le cadre d'une coopération entre plusieurs universités et/ou en collaboration avec des entreprises. Ces coopérations sont généralement régies par des contrats qui contiennent régulièrement des accords sur la confidentialité des résultats de la recherche. Ces **obligations de confidentialité** peuvent entraîner des limites quant aux **ORD**. Ces obligations peuvent notamment être prévues dans des contrats de coopération ou de licence, dans des *Non Disclosure Agreements (NDA)* ou dans des *Material Transfer Agreements (MTA)*. Les limites concernant les **ORD** peuvent également résulter **d'autres accords contractuels** régissant la gestion des données de recherche.

De telles stipulations contractuelles peuvent être en **contradiction avec la stratégie ORD** d'une institution du domaine des EPF ou avec sa mise en œuvre concrète dans des lois ou des directives internes. Dans ce cas, la question se pose de savoir si l'accord contractuel est valable. La liberté contractuelle régit l'élaboration du contenu d'un contrat. Des limites peuvent toutefois résulter de l'article 19 al. 2 CO, selon lequel un accord contractuel ne doit pas être contraire aux règles de droit strict, aux mœurs ou à l'ordre public. Le contrat est également nul s'il a pour objet une chose impossible, illicite ou contraire aux mœurs (article 20 al. 2 CO). Sont également illicites les contrats pour lesquels

¹¹⁰ cf. supra, 0.

une partie s'engage de façon excessive (article 27 al. 2 CC). Selon leur configuration, les dispositions relatives aux *ORD* peuvent relever du droit strict. Un contrat est **nul** au sens de l'article 19 et 20 CO, si son contenu est contraire à une disposition objective, de droit privé ou public, écrite ou non écrite, du droit strict suisse (fédéral ou cantonal)¹¹¹. Le caractère strict d'une disposition résulte de son interprétation¹¹².

Si un contrat entre les chercheurs et un partenaire contractuel contient un accord qui n'est pas conforme à la stratégie *ORD* de l'université, il convient de procéder à un examen en deux étapes : Dans un premier temps, il convient de vérifier si la norme potentiellement violée par le contrat est une **disposition légale** au sens des articles 19 et 20 CO. Tel est le cas, par exemple, de la loi sur les EPF ; toutefois, elle ne contient pas de dispositions relatives aux *ORD*. En ce qui concerne les directives internes, il convient de vérifier si elles peuvent être qualifiées de dispositions légales au sens des articles 19 et 20 CO. Dans un deuxième temps, il convient d'examiner si la **disposition** en question relève **du droit strict**. Si tel est le cas, le contrat est nul (article 20 al. 1 CO). Toutefois, selon la doctrine et la pratique dominantes, la nullité n'est pas automatique, mais ne s'applique que « lorsque cette conséquence juridique est expressément prévue par la loi ou découle du sens et du but de la norme violée »¹¹³. En outre, en vertu du principe de la nullité partielle, le champ de la nullité ne s'étend qu'aussi loin que le but protecteur de la norme violée l'exige.

Le but protecteur des dispositions relatives aux *ORD* ne devrait pas, en règle générale, exiger la nullité totale du contrat. Il serait plutôt conforme à la finalité de la disposition concernée que seules les dispositions du contrat qui contreviennent à la disposition pertinente de l'*ORD* soient considérées comme nulles. Les exceptions ne s'appliquent que si l'on peut supposer que l'ensemble du contrat n'aurait pas été conclu sans le contenu illicite¹¹⁴. Cela pourrait être le cas, par exemple, lorsqu'un contrat de coopération prévoit une obligation de confidentialité des données de recherche qui est nulle en raison d'une violation d'une disposition relative aux *ORD*, et que le contractant n'aurait pas conclu le contrat s'il avait su que les données de recherche devaient être rendues accessibles en tant qu'*ORD*.

Les **contrats de licence** peuvent également contenir des limites pour les *ORD*. Outre les obligations de confidentialité, les contrats de licence, par exemple, peuvent contenir certaines restrictions

¹¹¹ BSK OR I-MEISE/HUGUENIN, nbp. 106, art. 19 et 20 N 15 ; AHMET KUT/CHRISTOPH BAUER, in : Atamer/Furrer (Ed.), Handkommentar zum Schweizer Privatrecht, Obligationenrecht - Allgemeine Bestimmungen - Art. 1-183 OR, Zurich 2023, art. 20 N 13 ; BGer 4A_173/2010 du 22 juin 2010, E. 2.2.

¹¹² BSK CO I-MEISE/HUGUENIN, nbp. 106, art. 19 et 20 N 20 f. ; CHK OR-KUT/BAUER, nbp. 111, art. 20 N 14 ; BGE 143 III 600, E. 2.8.1.

¹¹³ BSK OR I-MEISE/HUGUENIN, nbp. 106, art. 19 et 20 N 54 et les références citées ; BGE 143 III 600, E. 2.8.1 ; BGE 134 III 438, E. 2.2 ; BGE 123 III 292, E. 2.e.aa.

¹¹⁴ BSK OR I-MEISE/HUGUENIN, nbp. 106, art. 19 et 20 N 64a ; CHK OR-KUT/BAUER, nbp. 111, art. 20 N 49 ; BGer 4C.156/2006 du 17 août 2006, E. 3.4 ; BGE 143 III 558, E. 4.1.1 ; BGE 124 III 57, E. 3.c et les références citées.

d'utilisation, géographiques ou temporelles, qui s'opposent aux *ORD*. Les stipulations en matière de diffusion et de publication des données, comme l'obligation de publier les données sur une plateforme spécifique, peuvent également entrer en conflit avec les dispositions relatives aux *ORD* des institutions du domaine des EPF.

5. Responsabilité

Si les chercheurs ne respectent pas les limites concernant les *ORD* et qu'il en résulte un dommage pour des tiers, les dispositions générales sur la responsabilité s'appliquent.

Dans les **rapports externes**, c'est-à-dire à l'égard des tiers, les institutions du domaine des EPF sont responsables, sans tenir compte de fautes de leurs employés, pour le dommage causé par leurs employés de façon illicite à des tiers dans l'exercice de leurs fonctions (article 3 al. 1 lu en combinaison avec l'article 19 al. 1 let. a de la Loi sur la responsabilité (LRCF) lu en combinaison avec l'article 5 al. 1 de la Loi sur les EPF). Certains domaines juridiques sont régis par des dispositions particulières (par exemple l'article 30 ss. LGG) qui priment sur la LRCF (article 3 al. 2 LRCF)), mais qui ne devraient guère être pertinentes ici. Parfois les contrats contiennent également des stipulations régissant les conséquences des violations du contrat, par exemple en fixant des pénalités contractuelles.

Dans les **rapports internes**, c'est-à-dire entre les employés et l'institution du domaine des EPF, les directives internes respectives s'appliquent, notamment les dispositions sur la mise à disposition de données de recherche en tant qu'*ORD* ainsi que les dispositions sur l'intégrité scientifique ainsi que les directives sur la procédure à suivre en cas de conduite scientifique inappropriée.

D. MISE EN ŒUVRE JURIDIQUE DES *ORD*

1. Remarque préliminaire

La Constitution contient les normes fondamentales de l'État. Une partie importante est constituée par les droits fondamentaux, qui garantissent aux individus des droits essentiels vis-à-vis de l'État. L'État n'est pas seulement l'État lui-même, mais aussi celui qui assume des tâches étatiques (article 35 al. 2 CF). Les **institutions du domaine des EPF** assument des tâches étatiques et sont **tenues de respecter les droits fondamentaux** dans leurs actions. Il convient de tenir compte de ces dispositions également lors de la mise en œuvre d'*ORD*.

Dès lors qu'il n'existe pas de restrictions légales et que des tiers n'ont pas de droits sur les données de recherche ou renoncent à l'exercice de ces droits, les données de recherche peuvent être rendues librement accessibles en tant qu'*ORD*. D'un point de vue juridique, **l'accès aux *ORD* peut être totalement libre**, c'est-à-dire sans conclusion d'un contrat de licence et sans acceptation des conditions

d'utilisation et donc sans que les utilisateurs soient soumis à des restrictions d'accès et d'utilisation des données.

En règle générale, l'opérateur d'une plateforme *ORD* ne mettra les données de recherche à disposition que sur la base d'un **contrat de licence**, afin de garantir le respect de certaines conditions (par exemple, l'indication de la source ou le respect de normes scientifiques). Ainsi, la prise de position du Conseil des EPF prévoit également que l'utilisation des *ORD* doit se faire sur la base d'une licence¹¹⁵.

2. Cadre constitutionnel

La mise en œuvre d'une stratégie *ORD* peut se faire de différentes manières. Pour une mise en œuvre efficace de l'approche, il peut être nécessaire d'obliger les chercheurs à rendre leurs données de recherche accessibles au public. Une telle obligation peut avoir des implications du point de vue des droits fondamentaux. Les droits fondamentaux tels que la liberté de la science, la garantie de la propriété et la liberté économique peuvent être concernés.

2.1. Droits fondamentaux pertinents pour les *ORD*

Le droit fondamental le plus important en rapport avec les *ORD* est la **liberté de la science** qui protège l'enseignement et la recherche scientifiques (article 20 CF)¹¹⁶. Les chercheurs concernés sont ceux qui se voient imposer un certain traitement des données de recherche par des dispositions relatives aux *ORD*. Face à cela, se trouve la liberté de la science des autres chercheurs et des membres de la communauté scientifique. Ils peuvent avoir besoin d'accéder à des données de recherche de tiers pour leur propre recherche. La question est de savoir si les données de recherche relèvent de la **garantie de la propriété** (article 26 CF). La garantie de la propriété protège tous les droits patrimoniaux de la propriété privée, lesquels comprennent outre les droits matériels, les droits immatériels¹¹⁷. La question de savoir si les données sont également couvertes par la notion de propriété en droit constitutionnel n'est pas encore clarifiée, mais la réponse est plutôt négative¹¹⁸. La **liberté économique** (article 27 CF) d'éventuels partenaires de coopération peut également être impactée. Elle protège la libre activité économique privée, en particulier le libre choix du métier, le libre accès à une activité professionnelle et son libre exercice (article 27 al. 2 CF)¹¹⁹. Au premier plan se trouvent ici les éléments du libre exercice de l'activité entrepreneuriale et de la liberté contractuelle. Une obligation de publication des données de

¹¹⁵ CONSEIL DES EPF, Open Research Data, Position du domaine des EPF, 5.

¹¹⁶ MAYA HERTIG, in : Waldmann/Besler/Epiney (Ed.), Basler Kommentar, Schweizerische Bundesverfassung (BV), Bâle 2015, art. 20 N 5.

¹¹⁷ BSK BV-VALLENDER/HETTICH, nbp. 116, art. 26 N 19 ; GIOVANNI BIAGGINI, in : Biaggini (Ed.), BV-Kommentar, Bundesverfassung der Schweizerischen Eidgenossenschaft, Zurich 2017, art. 26 N 12.

¹¹⁸ THOUVENIN, SJZ 2017, 21 ss., 21 ; BV Komm.-BIAGGINI, nbp. 117, art. 26 N 12.

¹¹⁹ BV-Komm., BIAGGINI, nbp. 117, art. 27 N 4 ; BSK BV-Uhlmann, nbp. 116, art. 27 N 4 faisant référence à BGE 131 I 333, E. 4 et BGE 137 I 167, E. 3.1.

recherche prive les partenaires de coopération de la possibilité de décider eux-mêmes de l'utilisation des données de recherche, par exemple par le biais d'une licence ou d'une vente à but lucratif.

2.2. Restriction des droits fondamentaux

Les droits fondamentaux ne sont pas absolus, mais peuvent faire l'objet de restrictions conformément à l'article 36 CF. La condition est qu'il existe une base légale, que la restriction soit justifiée par un intérêt public et proportionnée au but visé (article 36 CF). Ces dispositions sont à prendre en compte lors de l'élaboration concrète d'une stratégie *ORD*.

Il convient de tenir compte de l'exigence d'une **base légale** suffisante ; l'obligation de mise à disposition de données de recherche en tant qu'*ORD* devrait idéalement être ancrée dans une loi au sens formel du terme. La question de savoir si un ancrage dans des directives internes est suffisant devrait être examinée au cas par cas et dépend également de la portée de l'obligation. Un équilibre est à trouver entre l'**intérêt public** et l'intérêt des autres chercheurs et du public en général pour les données de recherche.

En ce qui concerne la **proportionnalité**, trois aspects doivent être examinés : l'aptitude, la nécessité et la proportionnalité au sens strict (caractère raisonnable). Les mesures attentatoires aux droits fondamentaux doivent être appropriées pour atteindre l'objectif d'intérêt public¹²⁰. L'atteinte à un droit fondamental doit en outre être nécessaire, c'est-à-dire qu'elle est limitée à ce qui est nécessaire pour remplir les objectifs d'intérêt public. En outre, l'intérêt public doit prévaloir sur les droits fondamentaux des personnes concernées qui s'y opposent, il convient donc d'examiner les intérêts en jeu. Le respect de la proportionnalité est susceptible d'être le point décisif lors de l'introduction d'une stratégie *ORD*. En ce qui concerne l'**aptitude** pour satisfaire à l'intérêt public, il convient de tenir compte d'aspects tels que l'accessibilité et les conditions dans lesquelles l'accès aux données est accordé. Moins les obstacles à l'accès aux données pour d'autres chercheurs sont importants, plus l'intérêt public est satisfait. En ce qui concerne la **nécessité**, il convient d'examiner jusqu'où l'obligation doit aller pour satisfaire à l'intérêt public poursuivi par la réglementation ; il convient de choisir respectivement la mesure la moins intrusive. Cela signifie que les droits fondamentaux des chercheurs et des partenaires de coopération concernés doivent être respectés autant que possible ; en font partie, outre la liberté de la recherche, également la garantie de la propriété et la liberté économique, qui sont impactées par une réglementation qui limite la libre disposition par des droits sur des biens immatériels éventuellement existants pour les données de recherche et par la protection des données de recherche en tant que secrets d'affaires¹²¹. Ces points devraient également être importants pour l'examen de la proportionnalité au sens strict.

¹²⁰ BV-Komm., BIAGGINI, nbp. 117, art. 5 N 21 faisant référence à BGE 136 I 29, E. 4.2 ; BSK BV-EPINEY, nbp. 116, art. 5 N 70.

¹²¹ cf. supra, B.1.5.

3. Contrats de licence

3.1. Objet

Par un **contrat de licence**, le donneur de licence autorise le preneur de licence à utiliser un bien immatériel selon l'étendue convenue¹²². Une rémunération (redevance ou royalties) ne fait pas partie des éléments objectivement essentiels du contrat, mais elle est régulièrement convenue¹²³. Un contrat de licence permet d'autoriser **l'utilisation de tous les types de biens immatériels**.

Il y a contrat de licence authentique lorsque le bien immatériel dont l'utilisation est concédée sous licence est protégé par un droit sur des biens immatériels (par exemple, un brevet ou un droit d'auteur). Un contrat de licence inauthentique régit l'utilisation d'un bien immatériel qui n'est pas (ou plus) protégé par un droit sur des biens immatériels¹²⁴, notamment l'utilisation du *know-how* (savoir-faire). Il s'agit notamment des informations qui sont protégées en tant que secrets de fabrication et d'affaires par l'article 6 LCD et l'article 162 CP contre l'utilisation non autorisée par des tiers. Il s'agit d'un contrat de licence mixte lorsqu'en plus de l'utilisation de biens immatériels protégés par un droit absolu, l'utilisation du *know-how* (complémentaire) est également autorisée¹²⁵. **Les contrats de licence** portant sur des données doivent généralement être qualifiés de **contrats de licence inauthentiques** ; si les données représentent des œuvres ou des prestations protégées par le droit d'auteur, il s'agit d'un contrat de licence mixte.

3.2. Forme

La conclusion d'un contrat n'est soumise à une exigence de forme que si cela a été prévu par la loi ou convenu par les parties (article 11 al. 1 et article 16 al. 1 CO). Étant donné que le contrat de licence est un contrat non réglementé par la loi (appelé contrat innommé), la loi ne prévoit **aucune exigence de forme**. Si les parties n'en ont pas convenu autrement, un contrat de licence peut donc également être conclu sous forme purement électronique, oralement ou par un comportement implicite¹²⁶.

¹²² Reto HILTY, *Lizenzvertragsrecht*, Bern 2002, 5 ss. ; BSK CO I-AMSTUTZ/MORIN, nbp. 106, introduction avt CO 184 ss. N 238 ; ROLAND VON BÜREN, in : David/von Büren (Ed.), *Schweizerisches Immaterialgüter- und Wettbewerbsrecht (SIWR)*, I/1, Grundlagen, Bâle 2002, 295.

¹²³ BSK CO I-AMSTUTZ/MORIN, nbp. 106, introduction avt CO 184 ss. N 238; EUGEN MARBACH/PATRIK DUCREY/GREGOR WILD, *Immaterialgüter- und Wettbewerbsrecht*, Bern 2017, para. 925 ; MAGDA STREULI-YOUSSEF, in : Streuli-Youssef (Ed.), *Schweizerisches Immaterialgüter- und Wettbewerbsrecht (SWIT)*, V/1, Bâle 2020, 22.

¹²⁴ ROBERT M. STUTZ/STEPHAN BEUTLER/MARC HOTTINGER, in : Stutz/Bleuler/Hottinger (Ed.), *Stämpfli Handkommentar, Designgesetz (DesG)*, Bern 2022, art. 15 N 12 ; CLAIRE HUGUENIN, *Obligationenrecht, Allgemeiner und Besonderer Teil*, Zurich 2019, para. 3792 ; HILTY, nbp. 122, 15.

¹²⁵ ROLAND FISCHER/LARA DORIGO, in : Weinmann/Münch/Herren (Ed.), *Schweizer IP-Handbuch, Intellectual Property – Konzepte, Checklisten und Musterdokumente für die Praxis*, Bâle 2021, § 17 Rz. 0.8.

¹²⁶ HILTY, nbp. 122, 275 ; VON BÜREN, nbp. 122, 332 ; SHK DesG-STUTZ/BEUTLER/HOTTINGER, NBP. 124, art. 15 N 21.

3.3. Contenu

Le droit des contrats repose sur le principe de la liberté contractuelle. Celle-ci comprend la liberté d'élaboration du contenu des contrats, appelé **liberté de contenu**¹²⁷. Dans le cadre des limites générales de la liberté contractuelle (notamment les articles 19 et 20 CO et l'article 27 CC)¹²⁸ les parties peuvent **librement élaborer des contrats de licence**. Cela s'applique également aux *ORD*. Les institutions du domaine des EPF peuvent ainsi définir librement les conditions des contrats de licence sous lesquels les données de recherche sont mises à disposition en tant qu'*ORD*.

Il est notamment possible d'octroyer la licence gratuitement (appelée « licence gratuite » ou « libre ») ou uniquement contre paiement d'une **redevance**. Les parties sont également libres de fixer les modalités de la redevance de licence. Dans la pratique, il existe de nombreuses variantes pour déterminer et calculer les redevances, telles que les redevances uniques, les paiements forfaitaires lorsque certains objectifs sont atteints constituant des jalons importants, les redevances périodiques, les redevances liées au chiffre d'affaires ou aux bénéfices et les licences à l'unité¹²⁹. Il arrive fréquemment que les parties associent un paiement forfaitaire lors de la conclusion du contrat (appelé « *downpayment* ») à une redevance périodique (par exemple, annuelle ou trimestrielle) en fonction du chiffre d'affaires¹³⁰.

L'étendue des **droits d'utilisation** accordés par la licence peut également être déterminée librement par les parties. L'utilisation peut notamment être limitée dans le temps (par exemple, pour une année seulement) ou dans l'espace (par exemple, uniquement dans un pays donné) ou à des fins spécifiques (par exemple, uniquement à des fins purement scientifiques, à l'exclusion de toute utilisation commerciale).

En outre, il est possible (et souhaitable) de préciser si le preneur de licence est autorisé à octroyer une **sous-licence** à des tiers leur permettant d'utiliser le bien immatériel. La sous-licence ne peut pas couvrir des pouvoirs plus étendus (mais moins étendus) que la licence principale. La question de savoir si le preneur de licence a le droit d'accorder une sous-licence lorsque le contrat de licence ne contient aucune disposition à ce sujet est controversée¹³¹ ; il conviendrait donc de régler la question également

¹²⁷ BSK CO I-MEISE/HUGUENIN, nbp. 111, art. 19 et 20 N 5 ss. faisant référence à BGE 115 II 237, E. 4.d ; PETER GAUCH/WALTER R. SCHLUEP/JÖRG SCHMID/SUSAN EMMENEGGER, Schweizerisches Obligationenrecht Allgemeiner Teil, Zurich 2020, Rz 626.

¹²⁸ cf. supra, C.4.

¹²⁹ Au sujet des différentes variantes : FISCHER/DORIGO, nbp. 125, § 17 Rz. 6.1 ; VON BÜREN, nbp. 122, 347 ss. ; HILTY, nbp. 122, 486.

¹³⁰ En détail sur le « *downpayment* » FISCHER/DORIGO, nbp. 125, § 17 Rz. 6.3 f.

¹³¹ HILTY, nbp. 122, 758 ff. ; VON BÜREN, nbp. 122, p. 314 ss. ; SHK DesG-STUTZ/BEUTLER/HOTTINGER, NBP. 124, Art. 15 N 15.

explicitement (et a fortiori) lorsque le preneur de licence n'est pas censé avoir le droit d'accorder une sous-licence.

4. Aspects du droit des cartels

Lors de la mise en œuvre des *ORD*, il convient de respecter certaines règles du droit de la concurrence. La Loi sur les cartels s'applique aux entreprises de droit privé et de droit public qui sont des acteurs économiques. En principe, les personnes privées ne sont pas soumises à la loi sur les cartels¹³². Le droit des cartels ne s'applique donc pas aux chercheurs qui rendent leurs données publiques. En revanche, les opérateurs de plateformes *ORD* devraient être soumis au droit des cartels.

Selon les conditions d'accès, il peut y avoir des problèmes du point de vue des opérateurs de plateformes *ORD* si un opérateur est qualifié d'entreprise ayant un pouvoir de marché relatif ou dominant le marché. Selon l'article 4 al. 2 de la LCart, une entreprise est considérée comme **dominante sur un marché** lorsqu'elle est en mesure de se comporter de manière essentiellement indépendante sur un marché. La part de marché est un facteur essentiel pour déterminer s'il y a position dominante ; sauf circonstances particulières¹³³ - celle-ci devrait être supérieure à 50 %, pour qu'on puisse considérer qu'il y ait une situation de dominance sur le marché¹³⁴. Comme les données de recherche sont collectées et traitées partout dans le monde, il est peu probable qu'une plateforme *ORD* soit qualifiée de dominante. Il est plus probable qu'il existe un pouvoir de marché relatif. Selon l'article 4 al. 2^{bis} LCart, une entreprise est considérée comme ayant un **pouvoir de marché relatif** lorsque d'autres entreprises sont dépendantes d'elle, de telle sorte qu'il n'y a pas d'alternatives suffisantes et raisonnables. Sous cet aspect, il convient également d'examiner si les données de recherche en question peuvent être considérées comme substituables. Les données de recherche qui font, par exemple, partie de l'état de la technique ou de la recherche et qui se trouvent donc aussi dans d'autres sources sont substituables. En ce qui concerne les données de recherche non substituables, il n'y a pas d'alternatives pour les autres chercheurs, raison pour laquelle il devrait y avoir un pouvoir de marché relatif lorsque ces données de recherche sont proposées par une institution de recherche en tant qu'*ORD*.

¹³² BERNHARD RUBIN/MATTHIAS COURVOISIER, in : Baker & McKenzie (Ed.), Stämpfli Handkommentar, Kartellgesetz (KG), Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen, Bern 2007, art. 2 N 9 ; RETO HEIZMANN/MICHAEL MAYER, in : Zäch et al. (Ed.), KG-Kommentar, Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen, Zurich 2018, art. 2 N 25.

¹³³ De telles circonstances particulières peuvent exister, par exemple, lorsque certaines données ne peuvent être collectées qu'auprès d'une institution de recherche et que celle-ci prévoit l'obligation de mettre des données à disposition exclusivement sur sa plateforme.

¹³⁴ JÜRIG BORER, in : Orell Füssli Kommentar, Wettbewerbsrecht I, Schweizerisches Kartellgesetz (KG) mit den Ausführungserlassen sowie einschlägigen Bekanntmachungen und Meldeformularen der WEKO, Zurich 2011, art. 4 N 19 ; SHK KG-ROLAND KÖCHLI/PHILIPPE M. REICH, nbp. 132, art. 4 N 38.

La détention d'un pouvoir de marché relatif ou d'une position dominante n'est pas illicite en soi, seuls certains **comportements abusifs** le sont (article 7 al. 1 f. LCart). L'article 7 al. 2 let. a LCart. peut être applicable. Si le détenteur d'une installation ou d'une information essentielle (*Essential Facilities*) **refuse l'accès aux tiers**, sans qu'il y ait pour cela des raisons objectives (*Legitimate Business Reasons*), il peut y avoir un refus illicite d'entretenir des relations commerciales. Il y a une installation essentielle chaque fois que l'accès à celle-ci est objectivement nécessaire pour opérer sur un marché en aval¹³⁵. Il convient d'examiner au cas par cas si une plateforme *ORD* est considérée comme une installation essentielle. Il n'y aurait violation de l'article 7 al. 2 let. a LCart que si l'accès à certaines données de recherche était restreint pour certaines catégories de personnes sans que des raisons objectives puissent être invoquées.

Un comportement abusif pourrait aussi consister en **l'imposition de prix ou de conditions commerciales inéquitable** (article 7 al. 2 let. c LCart), par exemple, si l'accès aux données est soumis à un prix (élevé) ou si l'accès à la plateforme *ORD* est soumis à des conditions particulièrement strictes qui diffèrent sensiblement des conditions applicables aux autres plateformes *ORD*. Il conviendrait de déterminer au cas par cas si ces éléments sont réunis. En ce qui concerne le montant de la redevance, il convient néanmoins de noter qu'une limitation de l'accès pour des raisons économiques par la perception d'une redevance est licite en vertu du droit des cartels, dans la mesure où il s'agit de compenser une charge financière liée à la mise à disposition des données. Il peut notamment s'agir de coûts relatifs au regroupement de jeux de données, à l'anonymisation ou à la création de l'interopérabilité.¹³⁶

5. Licences pour les *ORD*

5.1. Conclusion

La liberté contractuelle comprend également la liberté de conclure ou de ne pas conclure un contrat avec une partie, ce qu'on appelle la **liberté de conclure**¹³⁷.

D'un point de vue juridique, les fournisseurs d'*ORD* ne sont pas obligés de conclure un contrat de licence avec des tiers pour l'utilisation de données de recherche et ils sont en principe libres en cas de demande d'un tiers **de refuser l'octroi d'une licence**. Ils peuvent notamment prévoir de ne pas accorder de licences à certains tiers, par exemple des entreprises qui font de la recherche commerciale ou des

¹³⁵ MARC AMSTUTZ/BLAISE CARRON, in : Amstutz/Reinert (Ed.), Basler Kommentar, Kartellgesetz (KG), Bâle 2021, art. 7 N 181 et 248 ; RAMIN SILVAN GOHARI, Die Essential Facilities-Doktrin, sic! 2019, 533 ss., 535, 539, à chaque fois avec les références citées.

¹³⁶ ALFRED FRÜH, Datenzugangsrechte, sic! 2018 521 ss., 528 ss.

¹³⁷ BSK OR I-MEISE/HUGUENIN, nbp. 106, art. 19/20 N 8 faisant référence à BGE 129 III 35, E. 6.1 ; GAUCH/SCHLUEP/SCHMID/EMMENEGGER, nbp. 127, Rz 721 ss., 1102 ss.

universités de certains pays. Certaines restrictions à la liberté de conclure peuvent certes résulter du droit des cartels, les conditions pour une obligation de contracter sont toutefois strictes et ne seront remplies que dans de rares cas¹³⁸.

5.2. Rédaction

Les fournisseurs d'*ORD* sont en principe libres de rédiger leurs contrats de licence comme ils l'entendent¹³⁹. La liberté quasi totale au niveau du contenu permet d'aménager les contrats de licence les *ORD* de telle façon qu'ils soient conformes au concept des *ORD* et aux principes FAIR.

D'un point de vue juridique, il est tout à fait possible de faire dépendre l'octroi d'une licence *ORD* du paiement d'une **redevance**. En premier lieu, il s'agit d'une redevance unique qui est à verser lors de l'octroi de la licence et de l'accès aux données. Il est également envisageable d'exiger des entreprises le paiement d'une redevance et d'accorder des licences gratuites aux universités et aux autres institutions de recherche.

Les fournisseurs d'*ORD* peuvent librement déterminer l'**étendue des droits d'utilisation** accordés par une licence. Il est notamment envisageable de restreindre l'utilisation à des fins non commerciales. Il est également possible d'imposer des obligations supplémentaires aux preneurs de licence, telles que l'obligation de mettre également à disposition les connaissances acquises à partir des données ou les données générées par l'utilisation des *ORD*.

Les fournisseurs d'*ORD* devraient préciser si les preneurs de licence sont habilités à accorder des **sous-licences**. L'octroi d'une telle autorisation est possible mais semble peu judicieux si le fournisseur d'*ORD* souhaite conserver un certain contrôle sur l'utilisation des données de recherche. Les personnes intéressées par l'utilisation des données peuvent à tout moment obtenir une licence directement auprès du fournisseur d'*ORD*. Cette approche permet au fournisseur d'*ORD* de savoir qui est autorisé à utiliser les données de recherche.

5.3. Licences standard

Les contrats de licence peuvent être librement négociés et aménagés par les parties. S'ils utilisent cette liberté et concluent un contrat contenant des règles spécifiques pour le cas concret, il s'agit d'un **accord individuel**. Cependant, dans de nombreuses constellations, des contrats de licence standard sont utilisés, qui sont entièrement pré-rédigés par une partie et acceptés « *as is* » par l'autre partie. De tels

¹³⁸ cf. supra, D.4.

¹³⁹ Voir juste avant, D.5.2.

contrats de licence standard sont, par exemple, les licences *Creative Commons*¹⁴⁰ ou les licences développées par l'*Open Knowledge Foundation*¹⁴¹.

5.3.1. Open Database License

L'*Open Knowledge Foundation* a créé **trois licences standard pour les bases de données** : l'*Open Database License* (ODbL), l'*Open Data Commons Attribution License* (ODC-By) et l'*Open Data Commons Public Domain Dedication and License* (PDDL)¹⁴². Ces licences ne couvrent toutefois que les droits d'auteur et les droits *sui generis* sur les bases de données¹⁴³. Les autres droits, en particulier les éventuels droits découlant du droit de la protection des données ou d'une violation de l'obligation de garder les données secrètes,¹⁴⁴ ne sont pas pris en compte. Dans de nombreux cas, ces licences ne sont donc pas adaptées aux *ORD*.

L'*Open Data Commons Public Domain Dedication and License* (PDDL) autorise **l'utilisation des bases de données et de leurs contenus** de manière globale. Juridiquement parlant, il s'agit d'une combinaison d'une déclaration de renonciation et d'une licence. La PDDL comprend aussi bien les droits d'auteur et le droit *sui generis* sur la base de données que les droits sur le contenu de la base de données (article 2.2 PDDL). Avec la PDDL, le titulaire des droits introduit la base de données et son contenu dans le **domaine public** (*public domain*) (article 3.1 PDDL). Si cela n'est pas possible, parce que certains pays n'autorisent pas l'affectation au domaine public, le titulaire des droits renonce à ses droits d'auteur et au droit *sui generis* (article 3.2 PDDL). Si cela n'est pas non plus possible, parce que certains pays n'autorisent pas la renonciation aux droits d'auteur, le titulaire des droits accorde une licence globale à la base de données et à ses contenus (article 3.3 PDDL). La PDDL n'impose aux preneurs de licence aucune restriction dans l'utilisation de la base de données.

L'*Open Data Commons Attribution License* (ODC-By) autorise **l'utilisation de bases de données** protégées par le droit d'auteur ou par le droit *sui generis* sur les bases de données (article 2.1 f. ODC-By). Elle ne concerne toutefois que les droits sur les bases de données, et non les éventuels droits sur les **contenus des bases de données**, en particulier sur d'éventuels droits d'auteur ou droits voisins sur des œuvres ou des prestations contenues dans la base de données ; les droits relatifs à la protection des données ou à la protection de la personnalité ne sont pas non plus inclus dans la licence (article 2.4 ODC-By). L'ODC-By ne contient qu'une obligation d'« **attribution** » (article 4.3 ODC-By). L'octroi de **sous-licences** est exclu (article 4.4 phrase 1 ODC-By). Au lieu de cela, le donneur de licence offre aux

¹⁴⁰ Voir <<https://www.creativecommons.ch>> (dernière visite le 28 juin 2024).

¹⁴¹ Voir <<https://opendatacommons.org/licenses/>> (dernière visite le 28 juin 2024).

¹⁴² Voir <<https://opendatacommons.org/licenses/>> (dernière visite le 28 juin 2024).

¹⁴³ cf. supra, B.1.2. et B.1.3.

¹⁴⁴ cf. supra, B.3 et B.1.5.

tiers ayant reçu du preneur de licence la base de données (ou des parties de celle-ci) diffusée sous licence, sous une forme modifiée ou non, d'obtenir une *ODbL* (article 4.4 phrase 2 *ODC-By*).

L'**Open Database License (ODbL)** contient en partie les mêmes dispositions que l'*ODC-By*, mais prévoit des restrictions plus importantes. Comme l'*ODC-By*, l'*ODbL* permet **l'utilisation de bases de données** (article 2.1 f. *ODbL*). Comme l'*ODC-By*, elle ne concerne toutefois que les droits sur les bases de données, et non les éventuels droits sur les contenus des bases de données (article 2.4 *ODbL*). Outre l'obligation d'« **attribution** » (article 4.3 *ODbL*), l'*ODbL* contient également une obligation de « **share alike** » (article 4.4 *ODbL*). En outre, l'*ODbL* prévoit que les bases de données doivent être maintenues ouvertes (« **keep open** ») (article 4.7.a *ODbL*). Les tiers peuvent certes protéger par des conditions d'utilisation ou des mesures techniques l'accès et l'utilisation par des tiers d'une base de données qu'ils sont autorisés à utiliser conformément à l'*ODbL*, mais uniquement s'ils mettent à la disposition du destinataire de la base de données soumise à de telles restrictions également une copie de la base de données sans restrictions, appelée « *parallel distribution* » (article 4.7.b *ODbL*). Comme pour l'*ODC-By*, l'octroi de **sous-licences** est également exclu pour l'*ODbL* (article 4.8 *ODbL*).

5.3.2. Licence Creative Commons

Les licences *Creative Commons* sont un outil efficace pour déterminer de façon simple l'étendue des droits accordés aux utilisateurs en ce qui concerne une œuvre protégée par le droit d'auteur. Les licences *Creative Commons* ont acquis une grande reconnaissance et leur utilisation est recommandée par de nombreuses institutions publiques¹⁴⁵. Les titulaires de droits peuvent déterminer la manière dont leur contenu est exploité en choisissant parmi six catégories de licences *Creative Commons*.

La licence dite « **Attribution License** » (**CC BY**) est la plus permissive. Elle offre à chaque utilisateur la liberté de réutiliser les données, à condition de citer les titulaires originaux et d'indiquer si des modifications ont été apportées au contenu original. La licence dite « **Share Alike** » (**CC BY-SA**) exige la mention de la source et l'utilisation d'une œuvre nouvellement créée sur la base d'une œuvre existante sous la même licence. La licence dite « **Non commercial** » (**CC BY-NC**) prévoit les mêmes droits que la licence d'attribution (**CC-BY**), mais exclut toute utilisation à des fins commerciales. La licence dite « **No Derivatives** » (**CC BY-ND**) autorise l'utilisation commerciale, mais interdit toute modification des œuvres dérivées.

La **Creative Commons Zero License (CC0)** est une combinaison d'une déclaration de renonciation et d'une licence. Avec la *CC0*, l'« *Affirmer* » déclare **renoncer complètement** à ses droits d'auteur et

¹⁴⁵ Voir par exemple les recommandations de l'infrastructure Open Access pour la recherche en Europe (OpenAIRE), disponible sur <<https://zenodo.org/record/2574619>> (dernière visite le 27 mai 2024), qui recommande l'utilisation des licences Creative Commons CC BY 4.0 lorsque le matériel constitue une œuvre au sens de la LDA, et l'utilisation de la licence CC0 pour les données et les ensembles de données qui ne sont pas structurés comme des bases de données.

droits similaires (article 2 CC0). Ces droits sont définis de manière exhaustive dans la CC0 ; en font partie notamment (mais pas seulement) : droits d'utilisation issus du droit d'auteur, droits moraux de l'auteur, droits issus de la LCD, des droits *sui generis* sur les bases de données et droits similaires (article 1 CC0). Dans la mesure où cette renonciation n'est pas valable, l'« Affirmer » accorde une licence globale, gratuite et irrévocable concernant l'utilisation de tous les droits (article 3 CC0). Les données publiées sous une licence CC0 peuvent ainsi être utilisées, modifiées et réutilisées librement et sans restriction. La CC0 est un outil efficace pour créer la sécurité juridique, car elle indique clairement que les **contenus** ainsi désignés **peuvent être utilisés librement**. Elle a en outre l'avantage de résoudre le problème de l'« Attribution stacking », c'est-à-dire la nécessité de mentionner un grand nombre de jeux de données réutilisés. L'usage d'une licence CC0 donne ainsi aux utilisateurs la possibilité de regrouper plusieurs jeux de données sans avoir à se soucier de la mention des différents titulaires de droits.

5.3.3. Mise en œuvre

Les contrats de licence sont toujours conclus entre un (ou plusieurs) donneur(s) de licence et un (ou plusieurs) preneur(s) de licence. Le donneur de licence est le titulaire des droits qui peuvent être utilisés par le preneur de licence dans le cadre et sur la base du contrat de licence. Si le preneur de licence ne respecte pas les stipulations du contrat de licence, le donneur de licence peut faire valoir ses droits contractuels vis-à-vis du preneur de licence. Les contrats de licence contiennent parfois des dispositions relatives à la mise en œuvre des droits, par exemple sur l'annulation ou la résiliation en cas de violation du contrat ; si ces questions ne sont pas réglées par les parties, les dispositions générales du droit de la responsabilité contractuelle (article 97 ss. CO et article 192 ss. ainsi que l'article 367 ss. CO par analogie) s'appliquent. Cela vaut pour les contrats de licence individuels comme pour les contrats de licence standard. Comme il est proposé d'utiliser les licences **Creative Commons CC-BY et CC0** pour la mise à disposition de données de recherche en tant qu'ORD, seule la mise en œuvre de ces deux licences est brièvement esquissée ici.

La **Licence CC-BY** prévoit une série d'obligations contractuelles du preneur de licence, telles que l'obligation de mentionner le ou les auteur(s) ou l'obligation d'ajouter un avis relatif à la protection par le droit d'auteur (*copyright notice*) à la licence ou à une exclusion de responsabilité (*disclaimer of warranties*) (Sec. 3.a.1.A CC-BY). En outre, le preneur ne peut pas offrir l'objet de la licence à des conditions différentes ou supplémentaires (Sec. 2.5.B CC-BY). Si une obligation contractuelle n'est pas respectée, par exemple parce que l'auteur n'est pas mentionné, la licence prend fin automatiquement (Sec. 6.a CC-BY). Une action en justice pour demander **l'exécution des obligations contractuelles** est donc exclue, car le contrat de licence prend fin avec la violation et l'ancien preneur de licence ne peut plus être poursuivi en exécution du contrat dès lors qu'il est devenu caduc. Une action en **dommages-intérêts** est certes possible (section 6.b CC-BY), mais en général il n'y aura pas de dommage.



Contrairement à la licence *CC-BY*, la **licence CC0** ne prévoit pas d'obligations contractuelles pour le preneur de licence. Il ne peut donc pas enfreindre la licence *CC0* et la question de la mise en œuvre des droits contractuels ne se pose pas.

Le **titulaire des droits et le donneur de licence** ont le droit de **faire appliquer** les licences standard *CC-BY* et *CC0*. Le titulaire de droits des *ORD* est, en vertu de l'article 36 de la loi sur les EPF, l'institution du domaine des EPF ; il n'en va autrement que pour les droits d'auteur¹⁴⁶. C'est donc l'institution concernée du domaine des EPF qui a le droit de mettre en œuvre les licences standard. Si les *ORD* contiennent également des œuvres protégées par le droit d'auteur, une licence standard pour l'ensemble des données ne peut être accordée que conjointement par l'institution et les titulaires de droits d'auteur. Les deux (ou plusieurs) donneurs de licence peuvent toutefois agir de manière indépendante contre une violation du contrat et faire valoir leur part d'un éventuel dommage.

¹⁴⁶ cf. supra, B.2.

Template Guidelines for Open Research Data (ORD)

16. January 2025

Preamble

In May 2020, the ETH Board adopted an “Open Research Data Position of the ETH Domain” and established an “Open Research Data Programme”. This programme consists of five measures. Measure four concerns the legal basis for Open Research Data (ORD). Three objectives are being pursued as part of this measure: (i) identification of the (federal) legal obstacles to making research data accessible as ORD by researchers or the institutions of the ETH Domain; (ii) clarification of the responsibilities of researchers and the institutions of the ETH Domain; (iii) development of ORD guidelines that can be used as a common reference in the institutions of the ETH Domain.

These template guidelines have been developed to achieve objective (iii). The institutions of the ETH Domain may incorporate the provisions of these template guidelines into their existing guidelines on research data management or use them to develop separate ORD guidelines within their institution.

The (federal) legal obstacles to making research data available as ORD and the ORD-related responsibilities of researchers and institutions in the ETH Domain (objectives [i] and [ii]) are explained in the report “Open Research Data, Rechtliche Grenzen und Gestaltungsmöglichkeiten” of 31. January 2025. This report showed that not all research data can be made available as ORD. Swiss law contains various restrictions, some of which are general, while others are domain-specific. The most important general restrictions are:

- (i) Data protection law: research data may contain personal data, i.e. data relating to an identified or identifiable person (data subject); such data cannot be published as ORD without the consent of the data subjects.
- (ii) Copyright law: research data may contain copyright protected subject matter such as text, images, video footage, source code, and the like; such data may only be published as ORD with the consent of the copyright holder.
- (iii) Protection of trade secrets: research data may consist of or contain trade secrets. Such data may only be published as ORD with the consent of the trade secret holder.

Domain-specific restrictions vary according to the field of research. They are laid down in the Goods Control Act, the Information Security Act, the Human Research Act, the Geoinformation Ordinance, and in the Nuclear Energy Act, to name but a few of the most important laws and regulations. These restrictions usually apply to research activities in general, and not specifically to the making available of research data as ORD. Researchers should therefore be familiar with the restrictions that apply in their field of research. However, they need to be aware that these restrictions may also apply to the making available of research data as ORD, and that there may be more stringent restrictions if research data are to be made publicly available.

These guidelines aim to facilitate and promote the making available of research data as ORD by providing a set of rules to be applied. Although data ownership vests in the respective institution of the ETH Domain (see report “Open Research Data, Rechtliche Grenzen und Gestaltungsmöglichkeiten”, B.2), ORD-related decisions should be made by the researchers and the research group leaders based

on the ORD strategy of the respective institution, after consultation with the relevant internal service units, if necessary.

Art. 1 Scope

¹ These guidelines apply to all members of [institution of ETH Domain] involved in scientific research, including doctoral students [consider: and students], and to all fields of research.

² They only apply to Research Data and not to Scientific Code. However, Scientific Code must be made available with Research Data if such data cannot be analysed or reproduced without the corresponding Scientific Code.

Art. 2 Definitions

¹ Research Data are all data that the relevant scientific community deems necessary for validating research findings.

² Metadata are data that provide information about data.

³ Open Research Data (ORD) are Research Data that are publicly available, accessible, and reusable at no cost.

⁴ Scientific Code means machine-readable instructions created in a research project to analyse Research Data, to reproduce research findings from a data set, or to perform experiments.

⁵ FAIR Principles are internationally recognised guidelines to improve the Findability, Accessibility, Interoperability and Reuse of Research Data.

⁶ Research Group Leaders are [to be defined by institution of ETH Domain].

Art. 3 Publication of Research Data

¹ Research Data should be made available as ORD.

² After consultation with the researchers who contributed Research Data or Scientific Code, Research Group Leaders decide whether Research Data, associated Metadata and Scientific Code will be made available as ORD and whether such Data and Code will be made available immediately or after a reasonable embargo period.

Art. 4 FAIR Principles, Repository, and License

¹ Research Data that is made available as ORD must be published according to the FAIR Principles.

² After consultation with the researchers who contributed Research Data or Scientific Code, Research Group Leaders decide on which repository the Research Data is made available and what data format should be used.

³ If the repository does not require the use of a specific license, Researchers and Research Group Leaders jointly decide on the license to be used. The use of the “Creative Commons Zero License” (CC0) or the “Creative Commons Attribution License” (CC-BY) is recommended.

⁴ Research Group Leaders ensure that the making available of Research Data as ORD is addressed in the data management plan. They consider whether Research Data made available as ORD should also be stored in an additional repository or storage medium to ensure long-term preservation of the Research Data and to avoid dependence on a single repository.

Art. 5 Restrictions

¹ Research Group Leaders examine whether applicable laws, third-party rights, or contractual obligations, such as data protection laws, copyright law (including in Scientific Code), confidentiality obligations, and domain-specific regulations, restrict or prohibit the making available of Research Data as ORD.

² This examination must be carried out prior to making Research Data available as ORD. In case of doubt, Research Group Leaders must consult with the relevant internal service units.

Art. 6 Responsibility

Research Group Leaders are responsible for ensuring that the researchers in their group comply with these guidelines.