Universität Zürich[UZH]

CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

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, 16 January 2025

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

TABLE OF CONTENTS

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 (ITSL) 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 SchlT 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.), Stämpflis 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. 24*d* (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/HAAS/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 elements[17] 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, Innoweb 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 structure[24], 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 ARPAGAUS, 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-ARPAGAUS, 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-ARPAGAUS, 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-ARPAGAUS, 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 Jugenstrafgesetzbuch (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, BetmG, 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. 36*c* (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. 36*c* (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.), Stämpflis Handkommentar, Datenschutzgesetz (DSG), Bern 2021, Art. 5 N 13; GaborP. BLECHTA/LUCA DAL MOLIN/KIRSTEN WESIAK-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 regulations[61]. 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).

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.

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.

---

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.

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

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. 321bis 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. 118*b* 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 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.

---

65 Accord BENEDIKT VAN SPYK, in: Rütsche (ed.), Stämpflis 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.

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 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

---

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.

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

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

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 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.

[71] See above, B.3.

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 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

---

72 See above, B.3.

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

74 SR 810.12.

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 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.

---

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.

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.

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

---

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.

83 Federal Act on Geoinformation, SR 510.62.

84 Ordinance on Geoinformation, SR 510.620.

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.

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.

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.

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 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

---

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.

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

93 SR 732.1.

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.

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.

94 SR 732.11.

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 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

---

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.

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

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 services[101] and financial institutions[102] 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 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

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.

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.

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

---

104 MARK SCHWEIZER/HERBERT ZECH, in: Schweizer/Zech (eds.), Stämpflis 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".

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

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 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]

---

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.

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

108 See above, B.1.5.

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 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.

---

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

110 See above, B.3.

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]

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

---

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.

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.

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,

---

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 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]

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.

---

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

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.

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

---

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.

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 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]

---

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 RetoHILTY, 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.

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.

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.

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]

---

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.

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.

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 sublicence.

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 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

---

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.), Stämpflis 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.

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 JÜRG 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-RolandKÖCHLI/PHILIPPE M. REICH, fn. 132, Art. 4 N 38.

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]

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.

---

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.

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.

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.

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 licences[140] or the licences developed by the Open Knowledge Foundation.[141]

---

138 See above, D .4.

139 See above, D.5.2.

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).

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 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

---

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.

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). 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.

---

[145] See, for example, the recommendations of the Open Access Infrastructure for Research in Europe (OpenAIRE), 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.

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.