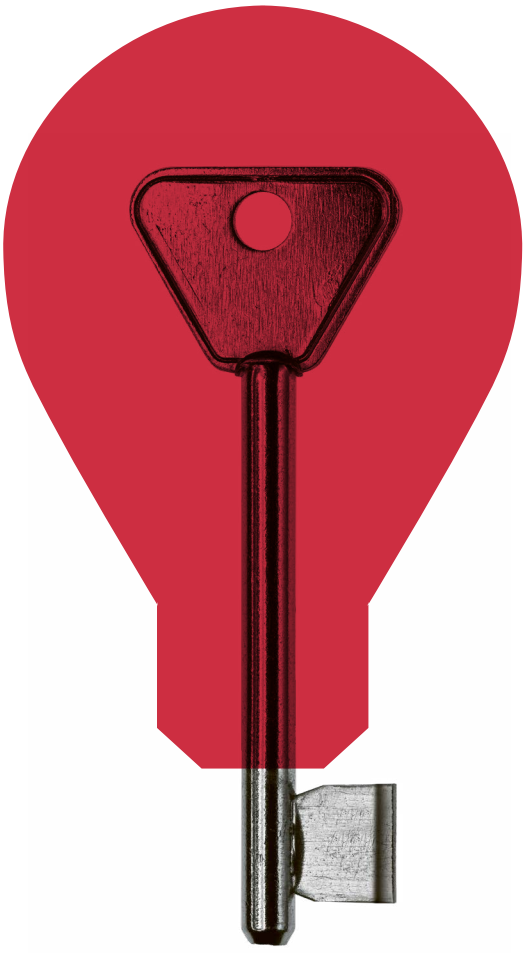
N

Monthly
Newsletter
October 2021

Intellectual Property
ICT

Schellenberg Wittmer



Data and Databases: Legal Framework and Market Relevance

Lorenza Ferrari Hofer, Peter Georg Picht, Roland Mathys, David Mamane

Key Take-aways

1.
Under Swiss law no ownership can be acquired in data. However, exclusive rights of use can apply to non-personal data through intellectual property protection and contractual agreements.

2.
Access to data can result from intellectual property, data protection and anti-trust law and is not necessarily unrestricted and for free. Swiss law lacks specific regulations for digital data.

3.
Any processing and transfer of personal data is ruled by the strict terms of data protection legislation. Strict responsibility and liability apply to anyone controlling or processing personal data.

1 Introduction

Data and databases dominate today's economic life. From a legal point of view, it is a matter of securing the rights to this "raw material", of looking at and using property and exclusive rights in them, and at the same time of recognising where the limits to dispose of the data lie.

Data can relate to individuals and allow to identify them or can be of a non-personal nature and be economically valuable merely for its content. A combination of both categories is common.

Data transactions, among others the access to and processing of data, their use on digital platforms and their cross-border transfer, need to be specifically addressed. With the development of digital technologies, big data and artificial intelligence, legislators worldwide have acknowledged the need of a legal framework for the commercial use of data.

Under Swiss law, no full-fledged ownership can be acquired in data.

2 Ownership in Data

Under Swiss law, **no full-fledged ownership** can be acquired **in data**. As a principle, any person having lawful access to data may also use it. No legal basis is necessary for this. Aimed at addressing the challenges of dealing with data in a digital society, Swiss law nevertheless provides for the possibilities to acquire factual ownership rights to data or to exercise a certain degree of control over them. Furthermore, access to, and use of, data may be restricted by the rights of third parties.

Under Swiss law, **personal data** is governed by the strict terms of the data protection legislation granting the data subjects mandatory rights of access and of use.

Non-personal data (including, for instance, machine-generated data) is governed by a number of norms conferring their owners a legal position that can come close to a property right. The focus is on the protection of manufacturing and trade secrets under Art. 162 of the Swiss Criminal Code (SCC) as well as under Art. 5 and 6 of the Act against Unfair Competition (UCA). Furthermore, certain provisions of criminal law (namely unauthorised data acquisition under Art. 143 SCC and unauthorised intrusion into a data processing system under Art. 143bis SCC) are also applicable. According to the law currently in force, the owners of non-personal data therefore enjoy relatively far-reaching legal protection.

Moreover, exclusive rights of use can apply to non-personal data that may qualify for protection as an intellectual property right, in particular as a copyright protected work. This may be the case for databases, digital works and software if they meet the specific requirements of copyright law. The legal discussion is particularly controversial around data generated by artificial intelligence or mathematical methods, which both play an important role in the solution of technical problems in all fields of technology and which today are frequently excluded from patentability.

The **introduction of an ownership** right in non-personal data has been discussed for some time. Following the report of the "Expert group on data processing and data security" of 17 August 2018, the Federal Council has decided against outright ownership in data. The Federal Council also seems hesitant to introduce a "sui generis" right in databases, as it already exists under EU law (Directive no. 96/9 on the legal protection of databases).

3 Access to Data

Even without full-fledged ownership, **factual control** over data can generate a high degree of exclusivity and protection. This begs the question of whether, when and how the law should grant mandatory rights of data access to non-controlling market participants. Such access rights can, in particular, result from rather general rules in intellectual property right law (e.g. copyright limitation for big data-based research, Art. 24d Copyright Act; CA), competition law (cf. case law like the Swiss Federal Administrative Court's decision *Terminals with Dynamic Currency Conversion (DCC)*, B-831/2011), or data protection law (e.g. a data subject's access right or right to data portability).

Increasing data-related competition law enforcement suggests that data controlling companies, especially if they are in a strong market position, check for the compliance of their data sharing policies and related agreements. The EU is about to go one step further and establish digital sector-specific regulation with its Digital Markets, Digital Services and Data Governance Acts (the "D-Package"), potentially to be followed soon by an even more comprehensive Data Act. As one of its many impacts on data-related rights and the data economy in the EU, the D-Package contains various stipulations **granting or ensuring data access** (e.g. access for advertisers, publishers and business users to their transaction data controlled by a digital gatekeeper, Art. 6 (1)(g)-(i) Digital Markets Act; data access for research purposes, Art. 31 Digital Services Act; prohibition of exclusive access arrangements, Art. 4 Data Governance Act).

However, it is important to note that data access rights **do not** necessarily guarantee **unrestricted or free access**. On the contrary, the default model is access under certain, context-specific conditions, such as a remuneration owed to the data controller, limitations in relation to the range of access-entitled market participants, or restrictions in the use of the accessed data. It is hardly surprising therefore, that the concept of FRAND (fair, reasonable, and non-discriminatory) access conditions to intangible assets, developed mainly in the licensing of standard-essential patents, is now being transferred to data access settings (cf., for instance, Art. 6(1)

(j) Digital Markets Act on FRAND access to search data for providers of online search engines). In a broader perspective, conditioned (as per FRAND or otherwise) data access rights are but one – albeit key – element of a developing and comprehensive data governance. The D-Package conceptualizes, amongst others, data altruism organizations and data intermediaries as further components of such governance regime also in Switzerland.

Factual control over data can generate a high degree of exclusivity and protection.

4 Use of and Contracting over Data

The swift evolution of data markets and a legal framework that is very much in the making create a challenging business environment. Therein, appropriately structuring data transactions by contractual means is paramount for success.

A legal status similar to ownership of non-personal data can be modeled by **contracts**. Appropriate contractual obligations remain, for instance, essential to maintain the protection of know-how, thus also safeguarding the value of the respective data portfolio and the attractiveness of its holder as a transaction partner.

Complex manufacturing and supply chain structures, among others for food, pharma and medical products require a high-performing data procurement system. Moreover, data collection and analysis through digital technologies become the basis of all future service offering and business models. Against this background, the establishment of data contracts between data suppliers, data receivers and data users should be given specific attention, both in respect of the assignment of rights in data and the permitted rights of use to such data.

Under Swiss law, the general legal provisions governing contracts apply to the assignment and the licensing of data and databases. No written form is required and parties can almost freely decide on the content of their contractual rights and obligations and the governing law. Flexible rules on arbitration render Swiss (law) based alternative dispute resolution an attractive option for data transactions.

The drafting of data contracts is a most challenging exercise. Their content can vary significantly: Contracts for the design for data and databases in software projects are structured differently from contracts on data connection and linking or from contracts on the exchange and comparison of data. If data used for commercial or research purposes is limited to use in specific countries, the extent of usage rights must be evaluated attentively.

5 Data Protection

If data relates to individuals or legal persons and allows to identify them, the processing of such personal data is only permitted if it complies with the principles of the data protection legislation. The enormous increase in access to, and automated use of, information entails a challenge to key privacy principles.

Data protection law is based on a number of principles setting **limits** to the processing of personal data in a data economy context: The principle of purpose limitation requires that personal data is only processed for the purposes indicated to the data subject at the time of data collection, obvious from the circumstances or provided for by law. If personal data is used for data mining and big data analysis, the processing purpose may not be fully determined in advance and will rarely be obvious nor communicated to the individual.

Pursuant to the transparency principle, each processing of personal data and in particular its purpose should be made transparent to the data subject. Given the huge number of data subjects regularly involved in mass data analysis, this principle will often not be complied with for practical reasons. The concept of proportionality requires that the processing of personal data is proportional to the envisaged purpose, e.g. that not more data is collected and processed than necessary. In a big data context, the opposite is often the case and vast amounts of data may be collected and retained for potential future analysis yet unknown at the time of collection. Finally, data related algorithms are often based on the identification of correlations rather than on causality. This can lead to wrong results in individual cases and thereby contravene the principle of data accuracy.

Data protection law may set limits to the processing of personal data.

Cross-border data transfers are often inherent to transactions in the data economy and may pose additional challenges. Data anonymization and aggregation may sometimes help to avoid the application of these data protection principles. However, some personal data is by its nature difficult to anonymize (e.g. health data), and anonymized data may often be re-identified, particularly by applying big data analysis techniques.

Most relevant is the responsibility and strict **liability** of private and public bodies controlling or processing personal data for the appropriate documentation of the data processing and the fulfilling of their obligations under the data protection law. Privacy infringements may entail damage compensation, penal prosecution proceedings and also severe fines.

6 Cybersecurity

Data digitalization has been entailing big challenges in terms of data security and requires the implementation of strict measures to prevent hacking, phishing, identity theft and other cybercrimes against personal, but also non-personal data. The massive increase of cyber incidents and data breaches has resulted in the perception that data may not only be an asset, but also a legacy.

Despite the fact that cybercrimes represent criminal or administrative offences prosecuted by law in Switzerland, legal liability is a key concern for anyone processing data. Individuals and entities affected by a data incident may turn to the provider of a defective product or service and third parties suffering damage as a consequence may hold the affected organization responsible for having failed to comply with the appropriate data security standards. In case of contractual relationships, the drafting of appropriate terms of use and liability provisions is essential.

7 Conclusions

Today, data management and data governance are strategic matters for every company, in particular in an international context. The digital transformation has entailed new chances for data transactions, in respect of which legal risks need to be addressed specifically. This will require a profound analysis of the legal issues around data as an economic asset.

Roland Mathys
Partner Zurich
roland.mathys@swlegal.ch

David Mamane
Partner Zurich
david.mamane@swlegal.ch

Dr. Lorenza Ferrari Hofer
Partner Zurich
lorenza.ferrarihofer@swlegal.ch

Grégoire Tribolet
Partner Geneva
gregoire.tribolet@swlegal.ch

Schellenberg Wittmer Ltd
Attorneys at Law

Zurich
Löwenstrasse 19
P. O. Box 2201
8021 Zurich / Switzerland
T +41 44 215 5252
www.swlegal.ch

Geneva
15bis, rue des Alpes
P. O. Box 2088
1211 Geneva 1 / Switzerland
T +41 22 707 8000
www.swlegal.ch

Singapore
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapore 049909
T +65 6580 2240
www.swlegal.sg