INFORMATION SHEET

Date: 2 May 2024

To: Nicolas Guyot (IPI)

CC: Anaic Cordoba (IPI)

From: Sylvain Métille, David Pressouyre (HDC)

Personal data and non-personal data

Translated from the original French version.

This translation has not been reviewed by HDC Avocats.

Av. de Sévelin 15
Case postale 851
CH-1001 Lausanne
T +41 (0)21 310 73 10
F +41 (0)21 310 73 11
www.hdclegal.ch

1. Introduction

The Swiss Federal Institute of Intellectual Property (IPI) commissioned the firm HDC to produce an information sheet aimed at the general public and small and medium-sized companies in particular to help them distinguish between personal and non-personal data. It also explains how to handle personal data when non-personal data is to be shared.

This information sheet is part of a wider series of recommendations and work carried out by the IPI to support the sharing of non-personal data between companies in the private sector (e.g. report drafted on access to non-personal data (in French), model agreements made available, public conferences). It is written in simple terms and without legal references to make it easier for the public to read and understand.

2. Personal data and non-personal data

2.1. Why should we differentiate between them?

Non-personal data is not subject to the strict provisions applicable to personal data under the Federal Act on Data Protection (FADP), the cantonal laws on the protection of personal data or the European legislation on this subject, that is, the General Data Protection Regulation (GDPR).

Hence, handling personal data involves implementing a certain number of measures to ensure the security and confidentiality of the data. By contrast, the European and Swiss authorities encourage the sharing of non-personal data, especially among companies in the private sector. The reason for this is to establish a free market for data, which will facilitate the creation of new services and help to boost companies' competitiveness.

On 1 March 2021, the IPI thus submitted a report to this effect on access to non-personal data in the private sector and made model agreements permitting such data sharing available to players in the sector.

2.2. Definition of personal data

Personal data is defined very broadly. The FADP considers personal data to be 'any information relating to an *identified* or *identifiable* natural person' (Art. 5 let. a FADP). It should be noted that some cantonal laws also include the data of legal entities, such as companies and associations, in this definition. The EU's GDPR defines personal data in the same way as the FADP.

A person is identified if the data establishes a direct link to the person (e.g. the person's full identity, consisting of their first name and last name). A person is identifiable if the data makes it possible to identify them indirectly in combination with other data (e.g. geolocation data or an IP address).

Sensitive personal data is a specific category of personal data. It consists of personal data relating to religious, philosophical, political or trade union-related views or activities, personal data about health, the private sphere or affiliation to a race or ethnicity, genetic data, biometric data that uniquely identifies a natural person, personal data relating to administrative and criminal proceedings or sanctions, and personal data relating to social assistance measures (Art. 5 let. c FADP). Increased attention must be given to such data. Similar provisions exist in cantonal and European law.

2.3. Definition of non-personal data

The concept of non-personal data is defined negatively by comparison with the concept of personal data. It thus means all data other than personal data.

The distinction between personal data and non-personal data thus depends on whether a person can be identified by means of the data in question. The larger the amount of data involved, the more likely it is that a person can be identified. If it is no longer technically possible to identify a person based on data, that data is not – or no longer – personal data. Technological developments are also making identification easier, which means that these concepts are evolving.

Although non-personal data is not subject to the laws on personal data protection, it is not completely unprotected. Other regulations may restrict the use and sharing of such data, such as provisions on intellectual property and the protection of secrets. Before sharing data, it is therefore advisable to ensure that it is not otherwise protected by legislation on secrecy, for example provisions on manufacturing or commercial secrecy (Art. 162 SCC, Art. 6 UCA), correspondence secrecy (Art. 179 SCC), official secrecy (Art. 320 SCC), professional confidentiality (Art. 321 SCC), research secrecy (Art. 321bis SCC), or postal and telecommunications secrecy (Art. 321ter SCC).

2.4. Some examples of personal and non-personal data

Personal data	Non-personal data
– Identification data (first name, last name, marital status) – Contact data (postal address, email address, telephone number) – Personal location data – Identification number (OASI number, credit card number, IBAN, number plate, reader number) – Extract from the criminal record – Medical files – Employer's letter of reference – IP addresses, cookies, digital footprint – etc.	– Aggregated statistical data – Anonymous data – Non-personal data generated by machines (not relating to people) – Maps or plans (not containing personal data) – Satellite images (not containing personal data) – Meteorological data – Agricultural or industrial production data (not containing personal data) – etc.

2.5. Can personal data become non-personal data?

Yes. Anonymising data makes it impossible to identify the person it relates to. Anonymised (or anonymous) data is thus data that can no longer be linked to a specific person. Anonymisation is an irreversible process. In other words, anonymous data is non-personal data because the link between the data and the person is definitively broken. There are a number of anonymisation techniques, such as aggregation, the addition of noise and substitution. What matters is that the result no longer allows the person to be identified.

Anonymous data differs from pseudonymous data, where one attribute, usually a unique attribute, is replaced by another in a record. A key or dictionary can be used to replace the original identifier (e.g. Mr Smith) with the

pseudonym (e.g. No 3178938), and vice versa. As a result, the person can still be identified indirectly, so pseudonymous data remains personal data, at least for the individual who has the key or the data that can be used to identify the people behind the pseudonyms. By contrast, this data is considered anonymous for individuals who do not have the key if identifying the person behind the pseudonym would involve disproportionate effort. We therefore speak of a relative concept of anonymisation (as opposed to an absolute concept whereby no one can identify the people concerned). The same data may thus be personal (pseudonymous) for the data controller and anonymous for third parties.

Conversely, anonymous data can become personal data when supplemented by other data.

2.6. What should I do if there is personal data?

If you wish to share non-personal data, you must ensure that it does not also include personal data. If it does, you have several options:

1. **Sort the data** – Firstly, you can communicate non-personal data only. Personal data is often unnecessary. This involves first sorting the data by identifying and then removing the personal data. In order to identify personal data, you need to ask yourself whether the data in question makes it possible either to identify one or more persons directly or to make those persons identifiable indirectly. If in doubt, we recommend that you consider the data to be personal data, in order to avoid any potential breach of the applicable legislation.

2. **Anonymise the data** – Secondly, it is possible to anonymise the personal data to be shared using a reliable and appropriate technique, for example by aggregating the data. In some cases, randomly replacing the identifying information can also make data anonymous. You should then ensure that the data is anonymous and the person or persons cannot be re-identified using other elements.

3. **Have a good reason for sharing** – Finally, if anonymisation is impossible, the communication of personal data is nonetheless possible in certain circumstances. This must be examined on a case-by-case basis. Good reasons may include the following:

    - The persons concerned have given their free and informed consent for the communication (Art. 31 para. 1 FADP).

    - The communication is necessary for the conclusion or performance of a contract, if the data processed concerns the contracting party (Art. 31 para. 2 let. a FADP).

    - Data is being processed exclusively for purposes not related to specific persons, for example for research, planning or statistical purposes. It is important to note that this exception does not only apply in the academic field but can also be applied in the commercial field, in particular if processing is carried out for statistical purposes. However, in this case, communication is only possible if: (1) data is anonymised as soon as the purpose of the processing permits or, if this is not possible, appropriate measures are taken to ensure that no persons can be identified, (2) any sensitive data is disclosed in a manner that does not allow the data subject to be identified or, if this is not possible, measures are taken to ensure that third parties only process the data for purposes not related to

specific persons, and (3) any published results are in a form that does not allow the data subjects to be identified (Art. 31 para. 2 let. e FADP).

- The personal data concerns a public figure and relates to their public activities (Art. 31 para. 2 let. f FADP).

If all three options are conceivable when data is being prepared for sharing, it is strongly recommended that this is considered at the planning stage. It is much easier to take steps at the time that the data files are collected or created to ensure that they do not contain any personal data or that such data is anonymised during processing. This means that there is no longer any need to take action when the question of data sharing arises, since only non-personal data is available.

*
* *

2.7. In a nutshell