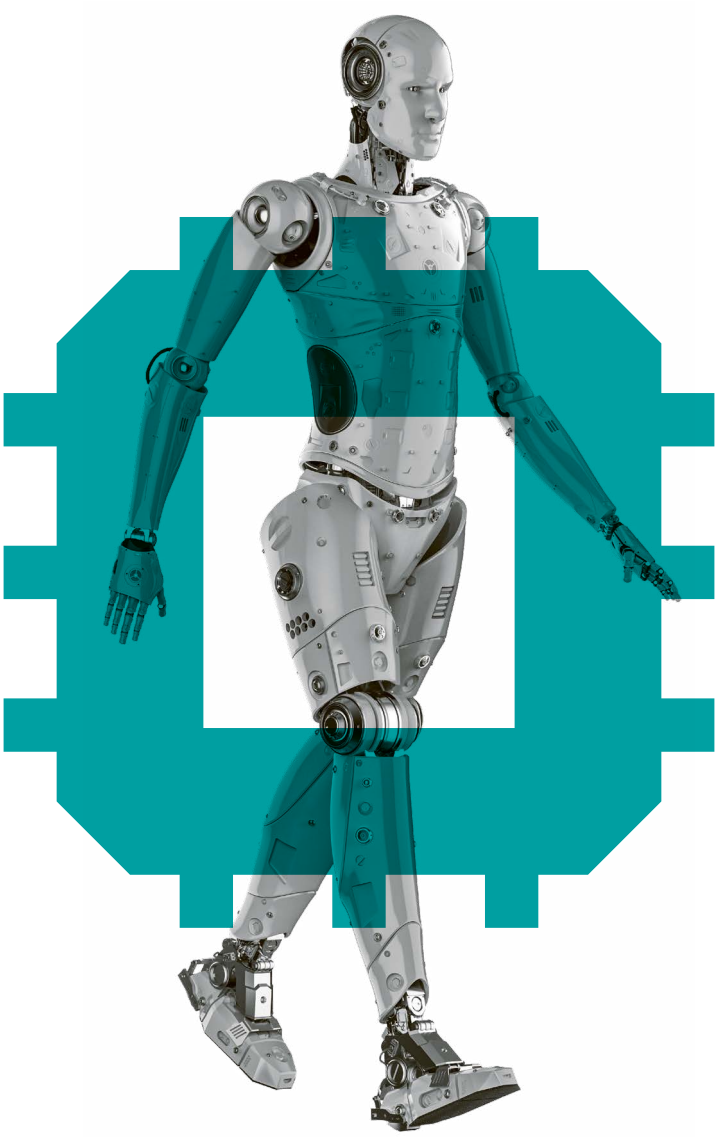
N

Monthly
Newsletter
December 2020

Information and Communication Technology

Schellenberg Wittmer



Data Protection in Daily Life

Claudia Jung, Samuel Klaus, Roland Mathys, Amalie Wijesundera, Floriane Zollinger-Löw

Key Take-aways

1.
Data processing takes place constantly and everywhere in daily life – often unnoticed. The interest in personal data is already immense today and will continue to grow.

2.
Useful services are increasingly offered free of charge. But "free of charge" does not mean "for free": The price is paid by disclosing one's data.

3.
Data protection law sets limits, but does not automatically provide comprehensive protection. Ultimately, it is up to the individual to decide for him- or herself what data processing shall be acceptable.

1 Introduction

The topic of data protection has become a hot issue these days. What was considered a marginal phenomenon of increasing digitalisation a few years ago is now of **fundamental importance** in Europe and beyond, and hardly any company can ignore it any longer. According to the annual Allianz Risk Barometer 2020, data protection breaches as part of cyber security have been classified for the first time as the **greatest business risk globally and in Switzerland**. This change in awareness is significantly due to stricter data protection legislations with drastic sanctions, particularly in the EU with the General Data Protection Regulation, but also in Switzerland with the revised Federal Act on Data Protection, which will soon come into force.

In stark contrast to this, there is a sense that the general public continues to be somewhat **undiscerning and careless** in their daily handling of personal data: data about oneself is freely disclosed, privacy notices and pertaining provisions in the general terms and conditions are accepted without much thought. People rarely reflect about what happens to their data and whether they agree with that. The reason for this might not be indifference, but rather a certain **lack of knowledge**.

The authors of this newsletter have taken this starting point as an opportunity to address the issue of data protection in daily life in a **Learning Lab** at this year's **Swiss Digital Days of digitalswitzerland** and to discuss this with a wider audience. An illustrative short **video** (in German) was produced for this purpose. This newsletter takes up this initiative and provides further information.

The use of data for marketing purposes may not be obvious.

2 Fundamentals and Basic Concepts of Data Protection

To start with, this section explains some key concepts of data protection law relevant in daily life:

- **Personal data**: This term covers information of any kind, content or form relating to one or more natural or legal persons. Examples of personal data are name, address, telephone number, e-mails or even the IP address. **Sensitive personal data** is a subgroup of personal data that is subject to stricter regulations. This includes, for example, data on religious views, health, race or the intimate sphere of a person.
- **Processing**: This term covers any handling of personal data. It includes not only activities such as the collection, retention, use or disclosure of personal data, but also activities such as the anonymization or deletion of such data.
- **Admissibility**: The processing of personal data is generally permitted under Swiss law. However, it is required that the provisions of the Federal Act on Data Protection and other laws (e.g. the unfair competition law when sending mass advertising or the Swiss Code of Obligations when processing employee data) are observed.
- **Principles**: The Federal Act on Data Protection provides for numerous data processing principles, the non-observance of which may constitute a privacy violation of the person concerned. The principle of **transparency** holds that the collection of personal data and its purpose must be evident to the data subject or apparent from the circumstances. The principle of **purpose limitation** requires that personal data be processed only for the purpose indicated at the time of collection, evident from the circumstances, or required by law. According to the principle of **proportionality**, personal data may only be processed to the extent that it is objectively appropriate and actually necessary for a specific purpose.
- **Rights of data subjects**: The primary right of the person subject to data processing is the right of information, whereby any controller of a data collection may be requested to provide information on data collected and on data processing operations. Other important rights include the right to block data (i.e. prohibit further processing), to prohibit disclosure to third parties, to rectify erroneous data and to demand the destruction of data.

3 Practical Example: Customer Card

A **retail chain** with a wide range of products including clothing, electronics, food and household items with branches throughout Switzerland and an online shop is introducing a **customer card with an app**. The use of the card and the app is voluntary. When registering, the user declares consent to the general terms and conditions of the retail chain. These general terms and conditions refer to the company's privacy notice.

The data the retail chain collects and processes for the above-mentioned purposes are **personal information and contact details** of the customers (first name, surname, address, e-mail address) as well as information on **purchasing behaviour** (time, place and purchased products).

The customer can show the card or use the app with every purchase and will then be **credited with points**. The points can be used to pay for purchases or participate in competitions. The purchases are continuously **analysed** in order to send customers targeted advertising and promotional vouchers. In the future, **artificial intelligence** shall be used for this analysis.

The retail chain sees an additional opportunity to commercialize the customer data by selling customer data to third parties worldwide, i.e. by **selling the data domestically and internationally**.

4 What is Permissible Under Data Protection Law?

Insofar as the customer is informed **transparently** about the collection and the purpose of the data, the company acts in accordance with data protection laws (provided that it actually complies with such information when processing and using the collected data). Generally, customers who register for a customer card are informed by means of the terms and conditions and the associated **data privacy notice**.

In dealing with personal data, one often senses a certain degree of carelessness.

In accordance with the principle of **purpose limitation**, the company may only use the data collected for the purposes that were indicated at the time of collection or apparent to the data subjects from the circumstances. In the case of a customer card, it seems clear from the circumstances that, when the card (or app) is used, the amount of the purchase is recorded and linked to the personal details of the card holder (otherwise it would not be possible to determine the number of points credited). However, any purposes beyond this (e.g. recording the date of the purchase, the individual products purchased, etc.) must be mentioned in the data privacy notice so that it is clear to the customer what data is collected and for what purposes it is used. The same applies to any selling of data (see below).

In particular, the use of personal data for **marketing purposes** may not be immediately apparent from the circumstances to the persons concerned. Transparent information in the privacy notice would therefore be necessary in this respect. If advertising material is to be delivered not only by post (e.g. references to campaigns, vouchers, catalogues), but also electronically (e.g. in the form of a newsletter, campaign e-mails), the requirements for electronic mass advertising in accordance with unfair competition law must also be complied with. In connection with the collection of personal data for the customer card (in particular the customer's e-mail address), it must therefore at least be pointed out that it is possible to refuse such advertising. If advertising is to be sent for offers from third parties or for completely different goods than those previously purchased by the customer, the customer's active consent is required.

But what about the **commercialization of data** – in other words, if the company collecting data from its customers also wants to sell it to other companies? Such "data trading" is not illegal per se, at least not as long as it is done respecting the data protection principles, in particular transparency and purpose limitation. Someone who provides his or her data to a retailer in order to benefit from a customer card does not have to anticipate that the retailer might sell the data collected to third parties who will use such data for their own purposes. The data provided may only be used by the retailer for the purposes originally disclosed (principle of **purpose limitation**). For such disclosure to be legally valid, it must be transparent, i.e. clear and comprehensible to those concerned by the disclosure (principle of **transparency**). An incidental mention in the "fine print", possibly hidden in a section with a different heading, would not suffice. The customer who registers to use the customer card must be aware of what will happen to and with his or her data - especially if such data is then sold to a third party.

When the data collected allows for an assessment of essential aspects of an individual's personality, this could constitute a **personality profile**. In this case, stricter regulations apply. Under the revised Federal Act on Data Protection, this is now regulated under the term **profiling**, which is understood as the automated processing of personal data in order to assess certain personal aspects of a natural person. In the case of automated analysis of purchasing data, this may apply if the analysis is aimed at an individual's purchasing behaviour or specific product preferences of a customer. If the processing exceeds a mere analysis, i.e. if – based on the analysis – an automated decision (e.g. by means of artificial intelligence) is being taken (e.g. whether a customer may benefit from certain special offers or discounts), the new data protection law provides for more extensive regulations for such **automated individual decisions**.

In order to verify what data is at hand and whether such data is correct, the customer may at any time request the responsible company to provide **information** about the data concerning him or her. If this data is incorrect, he or she may request that it be **corrected**. Within the framework of legal exceptions (e.g. archiving obligation), he or she can also request the **deletion** of such data at any time. If data is kept longer than necessary or legally required for the achievement of the purpose, this constitutes a breach of the principle of **proportionality**.

5 Conclusion

This brief everyday example of a customer card already shows how **many and manifold data processing operations** take place. While some of these may be obvious to the individual, others take place **unnoticed** and can lead to unpleasant surprises. The example also shows the immense **interest in the collection and processing of personal data**. This interest is not limited to the processes necessary for the actual processing purpose (e.g. processing of a purchase transaction or administration of credit points), but goes far beyond – for example, in case of shopping basket analysis using artificial intelligence or of actual data trading.

In such situations, the user is often offered a service or a certain comfort **free of charge**. Free of charge, however, does not mean that there is no "quid pro quo": The **"compensation"**

consists of data about oneself which is disclosed and then used for specific purposes.
The example further illustrates that not everything is permissible. Data protection law sets **limits**, but does not automatically provide comprehensive protection. It is ultimately the **responsibility of everyone** to decide whether and to what extent he or she allows his or her data to be disclosed and processed. This decision requires **basic knowledge of data protection principles** and the legal issues involved.

Roland Mathys
Partner Zurich
roland.mathys@swlegal.ch

Dr. Samuel Klaus
Partner Zurich
samuel.klaus@swlegal.ch

Vincent Carron
Partner Geneva
vincent.carron@swlegal.ch

Dr. Catherine Weniger
Counsel Geneva
catherine.weniger@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