Decentralizing privacy: Are distributed ledger technology systems designed to protect personal data?

20.06.2019

Key Takeaways

- **DLT systems must be reviewed under the point of view of data protection law;**
- **If Swiss data protection law is applicable, specific obligations are imposed on each participant in the DLT system (initiator of a transaction, the receiver or the validator);**
- **Breaches of data protection obligations may result in civil claims and/or entail criminal prosecution;**
- **To avoid legal consequences, basic principles of data protection law must be respected and data protection as well as technical measures must be considered when designing a DLT system.**

Distributed ledger technology (DLT) is one of the most remarkable and economically significant developments in digitalization. Inherent characteristics of these new technology systems include decentralized architecture, public visibility and subsequent immutability of data as well as an incontrovertible assumption of data accuracy. These very features demand a critical view of new technologies from the perspective of data protection law.

While data protection for centrally managed DLT systems ("private permissioned DLT systems") hardly deviates from that of conventional databases, data protection concepts reach their limits when it comes to open systems ("public permissionless DLT systems" or "public permissioned DLT systems").

This legal update primarily highlights the principles of Swiss data protection law and explores their compatibility with open DLT systems. In addition, it sets out some legal and technical approaches that address potential conflicts with data protection law.

Pestalozzi Rechtsanwälte AG
Feldeggstrasse 4
CH-8008 Zürich
T +41 44 217 91 11
zrh@pestalozzilaw.com

Pestalozzi Avocats SA
Cours de Rive 13
CH-1204 Genève
T +41 22 999 96 00
gva@pestalozzilaw.com

pestalozzilaw.com

Does Swiss law apply to open DLT systems?

DLT systems are, by their very nature, globally distributed networks in which cross-border data processing occurs regularly (e.g. if a Swiss DLT provider processes data of persons resident abroad and forwards it to foreign business partners). DLT systems can therefore generally be assumed to have an international connection.

Swiss data protection law does not contain any explicit provisions on its territorial scope. This means that neither the jurisdiction nor the applicable law is established from the outset for a specific DLT provider's data protection obligations as data processor.

Whether Swiss data protection law is applicable in international relations must be assessed separately for each provision of data protection law under discussion. Thereby it is important to distinguish between data protection provisions under public law and those under private law.

Data protection provisions under public law

If the data protection provision in question is made under public law (e.g. reporting obligation for cross-border data transmission (art. 6 para. 3 Federal Act on Data Protection (FADP), duty to inform (art. 7a/14 FADP), register of data collection (art. 11a FADP)), the FADP is only applicable to circumstances occurring in Switzerland due to the principle of territoriality. Such situations can be assumed if the place of processing of personal data is located in Switzerland, e.g. if the data controller is located in Switzerland, if the data is collected on a computer in Switzerland or if the data collection takes place in Switzerland.

A DLT provider domiciled in Switzerland is subject to the obligations arising from the aforementioned public law provisions. It is not possible to exempt the DLT provider by determining a different foreign law.

Data protection provisions under private law

With regard to private law provisions on data protection (e.g. right to information (art. 8 para. 1 FADP), breach of privacy through data processing), the question of when Swiss data protection law is applicable to international data processing is assessed according to the provisions of Swiss international private law (art. 139 Federal Code on Private International Law (CPIL)).

Accordingly, the civil law provisions of Swiss data protection law can be applied if (i) Switzerland's international jurisdiction is established (art. 129 CPIL or art. 2 and 5 no. 3 Lugano Convention), (ii) the domicile or habitual residence of the data subject or data processor is in Switzerland or the data processing takes place in Switzerland, (iii) the data processor had to foresee that the effects of the data processing would occur in Switzerland and (iv) the data subject exercises its right of choice in favor of Swiss law.

Swiss data protection law may therefore be applicable with regard to private law provisions even if data processing does not take place in Switzerland. In order to avoid a breach of privacy according to Swiss data protection law, the Swiss DLT provider must always observe data protection principles including, but not limited to, those on data processing (art. 4 FADP), data transfer abroad (art. 6 para. 1 and 2 FADP) and the protection of privacy according to art.

12 and 13 FADP.

Compliance with foreign data protection regulations

However, because the law grants the data subjects the right to demand application of the data protection provisions of their own country, the application of a foreign data protection law is not excluded if the data subject is domiciled or habitually resident abroad and the DLT provider is aware of this (art. 139 para. 3 in conjunction with art. 139 para. 1 lit. a CPIL). The data subject cannot legally waive this right in advance, e.g. by signing the general terms and conditions.

Alongside Swiss data protection law, foreign data protection standards may therefore also be applicable in individual cases. In particular, Swiss companies that process personal data (i) in order to offer goods or services to end customers in the European Union (EU) and/or (ii) to observe the behavior of persons affected by data processing may be forced to comply with the provisions of the European General Data Protection Regulation (GDPR).

When does the Federal Act on Data Protection apply to open DLT systems?

Application requirements

Factually, FADP applies when personal data is processed (art. 2 FADP). According to the legal definition, personal data is all information relating to an identified or identifiable person (art. 3 lit. a FADP). A person is identified when information clearly establishes the identity of that individual. The person is identifiable if that individual can be inferred on the basis of additional information.

It is not possible to generalize about whether data stored in a DLT system in the form of alphanumeric codes can be traced back to an identifiable person and thus qualify as personal data within the meaning of the FADP. Rather, the existence of personal data must be assessed on a case-by-case basis and in consideration of the specific circumstances. However, in accordance with the case law on dynamic IP addresses, data stored on DLT systems can be regarded as personal data if there is actual or legal access to additional information that enables the person concerned to be identified.

The second criterion of application of the FADP concerns the processing of data. Processing of data means any operation with personal data, irrespective of the means and procedures applied, in particular the collection, storage, use, modification, disclosure, archiving or destruction of personal data (art. 3 lit. e FADP).

Undisputedly, data processing in the sense of the law occurs when a new node is added to a blockchain (as a classic use case of a DLT), and the block is duplicated and saved again. Processors of this data are all participants in the DLT system, namely the initiator of a transaction, the receiver, and the party who validates a transaction under the consensus mechanism (so-called miner or validator).

Swiss law requires each of these processors to comply with the principles of transparency (recognizability of data procurement and its purpose), purpose limitation, proportionality,

correctness and security of the data (art. 4, 5 and 7 FADP). Finally, in the case of cross-border data disclosure to countries without adequate data protection, the processor must take sufficient measures to ensure appropriate protection (art. 6 FADP).

Rights of data subjects

While the processing principles of transparency and purpose limitation can easily be reconciled with DLT systems due to their technical structure, the exercise of data subjects' rights is particularly demanding.

Data subjects have a legal right to information, rectification, revocation and deletion. The right to information entitles data subjects to request information from the data controller as to whether data relating to them are being processed (art. 8 para. 1 FADP). Since public DLT systems do not have a central control body and thus no person responsible for data protection, the enforcement of the right to information is de facto impossible.

The other rights of data subjects are essentially aimed at correcting false, incomplete and/or redundant data (art. 5 FADP). Because data stored on DLT systems cannot be subsequently changed or deleted, the system does not allow rights of correction and deletion to be enforced.

Can open DLT systems be designed to comply with data protection regulations?

Although certain features of DLT are difficult to reconcile with data protection, there are data protection and technical instruments that can improve the data protection conformity of DLT systems.

First and foremost, the statutory presumption of the Federal Act on Data Protection must be considered, according to which no breach of privacy occurs during data processing if the data subject has made the data generally accessible and has not expressly prohibited such processing (art. 12 para. 3 FADP).

When individuals entrust their data to a DLT system, they agree that it may be published and used for participation in the DLT system.

By law, not every processing of personal data is legally problematic; only that which, due to a certain depth, leads to a breach of privacy (art. 13 para. 1 FADP). If the person concerned consents to data processing before using a DLT system, the specific processing of that individual’s data within the scope of application and to the extent of this consent is not unlawful.

In addition to these legal principles, the data protection conformity of a DLT system can also be guaranteed by technical measures (privacy by design).

The data protection problem of the subsequent immutability of the data can be countered, for example, by what are known as "chameleon hash functions". These enable data on a DLT system to be changed or deleted under certain conditions. Moreover, in certain circumstances it is possible to store data outside the DLT system and only store hash values of this data on the actual DLT system (off-chain storage).

Is there a need for action?

The discussion above demonstrates that DLT can provide effective data protection, provided the legal principles are correctly applied and appropriate technical measures are implemented.

Privacy by design seems especially important, i.e. the basic principles of data protection law should be taken into account when designing a DLT so that system compliance with data protection law can be achieved through inherent data protection functions within the system. Furthermore, particular attention must be paid to the preparation of the data protection concept and selection and implementation of appropriate technology.

Contributors: Lorenza Ferrari Hofer, Nando Lappert, Joseph Steiner

Michèle Burnier



Partner
Attorney at law

Pestalozzi Attorneys at Law Ltd
Cours de Rive 13
1204 Geneva
Switzerland
T +41 22 999 96 00
michele.burnier@pestalozzilaw.com

Oliver Widmer



Partner
Attorney at law
Head Financial Services

Pestalozzi Attorneys at Law Ltd
Feldeggstrasse 4
8008 Zurich
Switzerland
T +41 44 217 92 42
oliver.widmer@pestalozzilaw.com

Ludivine Boisard



Partner
Attorney at law

Pestalozzi Attorneys at Law Ltd
Cours de Rive 13
1204 Geneva
Switzerland
T +41 22 999 96 44
ludivine.boisard@pestalozzilaw.com