wenger & vieli
Attorneys at law

GUIDELINES

MARCH 2021

Wenger & Vieli Ltd.
Dufourstrasse 56
P.O. Box
CH-8034 Zurich

Office Zug
Metallstrasse 9
P.O. Box
CH-6302 Zug

T +41 58 958 58 58
guidelines@wengervieli.ch
www.wengervieli.ch

Data Breach

The digitalization that has occurred in recent years has brought enormous advantages and facilitations for society and the economy. However, it also poses risks in the form of hacker attacks or other methods of unlawful data acquisition ("data breaches"), which require a structured response in accordance with the law.

While the current Swiss Federal Act on Data Protection (FADP) does not stipulate any specific obligations in dealing with data breaches, the revised FADP (revFADP) contains an obligation for the data controller to notify the Federal Data Protection and Information Commissioner (FDPIC) as soon as possible about a data breach that is likely to result in a high risk to the personality or fundamental rights of the data subject. The revised FADP is expected to enter into force mid-2022 and does not contain any transitional provisions. Consequently, all provisions must be implemented as of the date of entry into force. It is therefore advisable to familiarize with the new obligations as early as now.

Data Breach

A data breach is a breach of security that results in personal data being inadvertently or unlawfully lost, deleted, destroyed or altered, or disclosed or made accessible to unauthorized persons. The breach may be caused by third parties or by employees who abuse their authority or act negligently. A data breach also exists if there is only the possibility that the personal data has been disclosed or made accessible to unauthorized persons. Consequently, it is not necessary to prove whether such access has actually taken place. For example, in the event of a loss of a data carrier, it is often hardly possible to assess whether the data stored on it was actually viewed or used by unauthorized persons. Therefore, the loss as such already constitutes a breach of data security.

Since a data breach can take many different forms, organizational measures must be taken to immediately detect a data breach. For the following incidents, a data breach must be investigated:

- Destruction of personal data which was not planned, commissioned or justified in this way;
- Lack of access to personal data despite the existence of the appropriate authorization;
- Loss or unintentional, unjustified modification of personal data;
- Unauthorized access to personal data;
- Unauthorized creation of copies or unauthorized transfer of personal data;
- Sending of e-mails to wrong recipients;
- Loss/theft of devices such as laptop, business cell phone, USB-drive or similar with unencrypted or insufficiently encrypted data;
- Publication of data on the Internet due to a technical error;
- Incorrect granting of access authorizations to personal data;
- Disposal of documents, audio or video media not in compliance with data protection requirements.

CLAUDIA KELLER
LL.M. | Counsel | Attorney at law
c.keller@wengervieli.ch
T +41 58 958 53 47

MICHAEL TSCHUDIN
Dr. iur. | Partner
m.tschudin@wengervieli.ch
T +41 58 958 55 47

DOMINIQUE ROOS
MLaw | Attorney at law
d.roos@wengervieli.ch
+41 58 958 55 47

MARCEL BOLLER
Dr. iur. | Attorney at law
m.boller@wengervieli.ch
T +41 58 958 55 63

GUIDELINES AS PDF:
https://www.wengervieli.ch/en-us/publications?typ=guidelines

Disclaimer: The information contained in this document is intended for general information purposes only and does not constitute legal or tax advice. This content is not meant to replace individual advice from competent professionals in a specific case. © Wenger & Vieli Ltd., 2021

Not every breach of data security results in an obligation to notify the same. Rather, a notification to the FDPIC must only be made if the data breach poses a high risk to the personality or fundamental rights of the data subjects. This restriction is intended to prevent insignificant breaches from being subject to a notification obligation. Whether a high risk to the personality or fundamental rights of the data subject has existed or continues to exist must be examined or assessed by the company itself in a comprehensible manner.

To ensure that the right measures can be taken immediately when a data breach becomes known, an emergency plan ("incident response plan") must be drawn up as a preparatory measure to enable rapid and targeted action in the event of an incident.

Incident Response Plan

The revFADP stipulates that a notification must be made "as soon as possible". Among other things, the incident response plan must define the various procedures for an emergency and its follow-up. This is done most simply in the form of a process flow diagram, in which it is specified who has to inform whom at which stage of the procedure. The incident response plan, which is usually of great importance especially in the case of IT data breaches, must address the following topics:

- Internal notification obligations in the event of a data breach:
  Who bears the main responsibility for handling a data breach and which bodies are to be involved and when;
- Measures for establishing the facts:
  What steps are to be taken to clarify the incident and which internal and external bodies are available for this purpose;
- Accompanying communication measures:
  Principles for internal and external communication about the data breach;
- Obligation to report, yes or no:
  Determination of the relevant decision criteria for or against a notification to the FDPIC;
- Follow-up:
  Principles for follow-up such as analysis of the data breach process flows, clarification with regard to optimization potential, examination of the introduction of further preventive measures.

In order to prevent a data breach to the maximum extent possible from the outset, data protection management tailored to the company and the risk of personality violations and financial damage associated with the specific data processing is necessary. But even a sophisticated data protection management system does not provide absolute protection against data breaches. In the event of a data breach, it is important that the procedures defined in the incident response plan are followed and function properly. This requires regular training of employees as well as regular review of the incident response plan, even if no data breach has occurred for a longer period of time. Data breaches are not only a purely legal matter, but the commitment of business-relevant resources (both financial and time-related) and accompanying communication measures must also be taken into account.