wenger & vieli
Rechtsanwälte

GUIDELINES

MÄRZ 2021

Wenger & Vieli AG
Dufourstrasse 56
Postfach
CH-8034 Zürich

Büro Zug
Metallstrasse 9
Postfach
CH-6302 Zug

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

Datenschutzverletzung

Die in den letzten Jahren erfolgte Digitalisierung brachte enorme Vorteile und Erleichterungen für die Gesellschaft und die Wirtschaft. Sie birgt jedoch auch Risiken in Form von Hackerangriffen oder sonstigen Methoden der rechtswidrigen Datenbeschaffung («Data Breach»), bei welchen strukturiert und gesetzesgemäss reagiert werden muss.

Während das heutige schweizerische Datenschutzgesetz (DSG) keine speziellen Pflichten im Umgang mit Datenschutzverletzungen statuiert, enthält das revidierte Datenschutzgesetz (revDSG) eine Verpflichtung des Verantwortlichen, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) eine Verletzung der Datensicherheit, welche voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, so rasch als möglich zu melden. Das revidierte DSG wird voraussichtlich Mitte 2022 in Kraft treten und enthält keine Übergangsbestimmungen. Sämtliche Bestimmungen müssen folglich ab Zeitpunkt des Inkrafttretens umgesetzt werden. Daher ist es ratsam, sich bereits jetzt mit den neuen Verpflichtungen vertraut zu machen.

Datenschutzverletzung

Eine Datenschutzverletzung ist eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Die Verletzung kann dabei durch Dritte oder auch durch Mitarbeiter, die ihre Kompetenzen missbrauchen oder fahrlässig handeln, erfolgen. Eine Datenschutzverletzung liegt auch dann vor, wenn lediglich die Möglichkeit besteht, dass die Personendaten Unbefugten offengelegt oder zugänglich gemacht wurden. Es muss folglich nicht nachgewiesen werden, ob ein solcher Zugang tatsächlich stattgefunden hat. So ist es beispielsweise bei einem Verlust eines Datenträgers oft kaum möglich, zu beurteilen, ob die darauf gespeicherten Daten tatsächlich durch Unbefugte eingesehen oder verwendet wurden. Daher stellt bereits der Verlust als solches eine Verletzung der Datensicherheit dar.

Da eine Datenschutzverletzung in ganz unterschiedlichen Formen auftreten kann, müssen organisatorische Massnahmen getroffen werden, um eine Verletzung des Schutzes personenbezogener Daten sofort zu erkennen. Bei folgenden Vorfällen ist eine Datenschutzverletzung zu prüfen:

- Vernichtung von Personendaten, ohne dass dies so geplant, in Auftrag gegeben oder gerechtfertigt war;
- Fehlende Zugriffsmöglichkeiten auf Personendaten trotz des Vorliegens der entsprechenden Berechtigung;
- Verlust oder ungewollte, nicht gerechtfertigte Änderung von Personendaten;
- Unbefugter Zugriff auf Personendaten;
- Unbefugtes Erstellen von Kopien oder unbefugter Transfer von Personendaten;
- Versand von E-Mails an falsche Empfänger;
- Verlust/Diebstahl von Geräten wie Laptop, Geschäftshandy, USB-Stick oder Ähnliches mit unverschlüsselten oder nicht ausreichend verschlüsselten Daten;
- Veröffentlichung von Daten im Internet aufgrund eines technischen Fehlers;
- Fehlerhafte Erteilung von Zugriffsberechtigungen auf personenbezogene Daten;
- Nicht datenschutzgerechte Entsorgung von Unterlagen, Ton- oder Bildträgern.

CLAUDIA KELLER
LL.M. | Counsel | Rechtsanwältin
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 | Rechtsanwältin
d.roos@wengervieli.ch
+41 58 958 55 47

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

GUIDELINES ALS PDF:
https://www.wengervieli.ch/de-ch/publikationen?typ=guidelines

Nicht jede Verletzung der Datensicherheit hat eine Pflicht zur Meldung derselben zu Folge. Vielmehr muss eine Meldung an den EDÖB nur erfolgen, wenn die Verletzung der Datensicherheit ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen birgt. Diese Einschränkung soll verhindern, dass unbedeutende Verletzungen einer Meldepflicht unterliegen. Ob ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person bestanden hat oder weiterhin besteht, muss das Unternehmen selbständig und nachvollziehbar prüfen bzw. abschätzen.

Damit bei Bekanntwerden einer Datenschutzverletzung umgehend die richtigen Massnahmen ergriffen werden können, muss als Vorbereitungsmassnahme ein Notfallplan erarbeitet werden, der im Ernstfall ein rasches und zielgerichtetes Handeln ermöglicht.

Notfallplan

Das revDSG schreibt vor, dass eine Meldung «so rasch als möglich» zu erfolgen hat. Der Notfallplan hat unter anderem die verschiedenen Abläufe für den Ernstfall und dessen Nachbearbeitung zu definieren. Dies erfolgt am einfachsten in Form eines Prozessablaufdiagramms, in welchem festgelegt wird, wer wen in welchem Verfahrensstadium zu informieren hat. Der Notfallplan, der in der Regel vor allem bei IT-Datenschutzverletzungen von grosser Bedeutung ist, hat folgende Themenbereiche zu regeln:

- Interne Notifikationspflichten im Falle einer Datenschutzverletzung:
  Wer trägt die Hauptverantwortung für die Bearbeitung einer Datenschutzverletzung und welche Stellen sind wann beizuziehen;
- Massnahmen zur Sachverhaltsfeststellung:
  Welche Schritte sind zur Abklärung des Vorfalls einzuleiten und welche internen und externen Stellen stehen hierfür zur Verfügung;
- Flankierende Kommunikationsmassnahmen:
  Grundsätze zur internen und externen Kommunikation bezüglich der Datenschutzverletzung;
- Meldepflicht, ja oder nein:
  Festlegung der relevanten Entscheidungskriterien für oder gegen eine Meldung an den EDÖB;
- Nachbearbeitung:
  Grundsätze zur Nachbearbeitung wie Analyse der Data Breach Prozessabläufe, Abklärung hinsichtlich Optimierungspotenzial, Prüfung der Einführung weitergehender Präventionsmassnahmen.

Um einen Data Breach von vornherein soweit wie möglich zu verhindern, ist ein auf das Unternehmen und das mit der konkreten Datenbearbeitung zusammenhängende Risiko für Persönlichkeitsverletzungen und finanzielle Schäden angepasstes Datenschutzmanagement notwendig. Aber selbst ein ausgeklügeltes Datenschutzmanagementsystem bietet keinen absoluten Schutz vor Datenschutzverletzungen. Im Falle einer Datenschutzverletzung ist es wichtig, dass die im Notfallplan definierten Abläufe eingehalten werden und funktionieren. Dies bedingt eine regelmässige Schulung der Mitarbeitenden wie auch eine regelmässige Überprüfung des Notfallplans, selbst wenn während längerer Zeit keine Datenschutzverletzung aufgetreten ist. Datenschutzverletzungen sind sodann nicht nur eine rein rechtliche Angelegenheit, sondern es gilt auch die Bindung von geschäftsrelevanten Ressourcen (sowohl finanzieller wie zeitlicher Natur) sowie flankierende Kommunikationsmassnahmen zu berücksichtigen.