

**Claudia Keller**

LL.M., Rechtsanwältin, Counsel  
T +41 58 958 58 58  
c.keller@wengervieli.ch

**Dr. iur. Michael Tschudin**

Rechtsanwalt, Partner  
T +41 58 958 53 36  
m.tschudin@wengervieli.ch

Wenger & Vieli AG Rechtsanwälte  
CH – 8034 Zürich  
www.wengervieli.ch

**Claudia Keller****Dr. iur. Michael Tschudin**

Aufgrund einer Anzeige des Online-Magazins Republik hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte EDÖB Ende März 2021 ein formelles Verfahren gegen die Betreiberin einer Plattform für ein digitales Impfregister eröffnet, um insbesondere Informationen zu angeblich stattgefundenen Datenverletzungen zu erhalten. Es steht der Verdacht im Raum, dass personenbezogene Daten der Plattformnutzer von Unbefugten relativ einfach eingesehen und sogar manipuliert werden konnten. Die Abklärung der Vorwürfe ist deshalb von hohem Interesse,

# DAS REVIDIERTE SCHWEIZER DATENSCHUTZGESETZ – FOKUS MELDEPFLICHT VON DATENVERLETZUNGEN

weil über die Plattform bereits mehrere hunderttausend Nutzer ihre Gesundheitsdaten, das heisst besonders schützenswerte Personendaten, in diesem digitalen Impfregister gespeichert haben.

Für die sich in Abklärung befindlichen Datenverletzungen dieses digitalen Impfregisters ist im geltenden Datenschutzgesetz (DSG) keine Meldepflicht statuiert. Im revidierten Datenschutzgesetz, das vom Schweizer Parlament im Herbst 2020 verabschiedet wurde und voraussichtlich Mitte 2022 in Kraft tritt, findet sich hingegen neu eine Meldepflicht für Datenschutzverletzungen. Wir nehmen den aktuellen Fall zum Anlass, diese neue Meldepflicht und damit zusammenhängende Massnahmen näher zu analysieren.

## Wann spricht man von einer Datenschutzverletzung?

Eine Datenschutzverletzung liegt vor, wenn Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet, verändert, Unbefugten offengelegt oder zugänglich gemacht werden. Die Gefahr einer Verletzung geht nicht nur von böswilligen Dritten wie bspw. Hackern aus, sondern auch von Mitarbeitenden, die ihre Kompetenzen missbrauchen oder fahrlässig handeln oder ungenügenden technischen und organisatorischen Sicherheitsmassnahmen.

## Wann und wie schnell muss eine Datenschutzverletzung dem EDÖB gemeldet werden?

Die Meldepflicht besteht dann, wenn mit der Datenschutzverletzung ein hohes Risiko für Persönlichkeitsrechte der betroffenen Personen verbunden ist. Die Einsichtnahme und Gefahr der Manipulation von Impf- und Gesundheitsdaten betroffener Personen würde unter dem neuen Recht aller Voraussicht nach als hohes Risiko für die Persönlichkeitsrechte eingestuft und somit würde eine Melde-

pfllicht bejaht. Nach der europäischen Datenschutzgrundverordnung (DSGVO) hat die Meldung innert 72 Stunden, gemäss revidiertem DSG «so rasch als möglich» zu erfolgen. Da je nach den betroffenen Personen Meldepflichten in verschiedenen Ländern bestehen können, sollte die Abklärung der Meldepflichten sowie der entsprechende Inhalt koordiniert werden.

Wichtig zu wissen: Eine Datenschutzverletzung ist auch dann gegeben, wenn nur die Möglichkeit besteht, dass die betreffenden Personendaten Unbefugten offengelegt oder zugänglich gemacht wurden. Ein Nachweis, dass ein Zugang stattgefunden hat, ist nicht Voraussetzung für das Bejahen einer Meldepflicht.

## Wie kann ich eine Datenschutzverletzung verhindern?

Vorweg: einen 100%igen Schutz wird es nie geben. Aber da eine Datenschutzverletzung in ganz unterschiedlichen Formen auftreten kann, müssen einerseits organisatorische Massnahmen getroffen werden, um eine Verletzung des Schutzes personenbezogener Daten umgehend entdecken zu können. Es sind also organisatorische und technische Massnahmen zu implementieren, die sicherstellen, dass nicht datenschutzkonforme Bearbeitungstätigkeiten oder Datenverluste bemerkt werden.

## Wie bereite ich mich auf den Ernstfall vor?

Damit im Ernstfall keine Verzögerungen auftreten, ist es unerlässlich, die konkrete Vorgehensweise für den Ernstfall zu planen und Verantwortlichkeiten zuzuweisen. Ein solcher Notfallplan sollte die verschiedenen Abläufe für den Ernstfall und dessen Nachbearbeitung festlegen und mindestens folgende Themen abdecken:

- Interne Notifikationspflichten im Falle einer Datenschutzverletzung: Wer trägt die Hauptverantwortung für die Bearbeitung einer Datenschutzver-

letzung und welche Stellen sind wann beizuziehen.

- Massnahmen zur Sachverhaltsfeststellung:  
Welche Schritte sind zur Abklärung des Vorfalles einzuleiten und welche internen und externen Stellen stehen hierfür zur Verfügung.
- Flankierende Kommunikationsmassnahmen:  
Festlegung der 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:  
Rückwirkende Fallanalyse und Überprüfung der Prozessabläufe. Wird Optimierungspotenzial erkannt, Evaluation und Implementierung weitergehender Präventionsmassnahmen.

Diese organisatorischen Massnahmen sollen im Ernstfall gewährleisten, dass die gesetzlichen Pflichten gegenüber der zuständigen Datenschutzstelle umgesetzt werden. Ausserdem sollte die Analyse einer Datenschutzverletzung vertraulich durchgeführt werden, um die Rechte der entsprechenden betroffenen Datensubjekte zu respektieren und die Verteidigung vor möglichen Ansprüchen gegen das Unternehmen optimal vorzubereiten. Eine Meldung an den EDÖB kann der erste Schritt in einem langwierigen Prozess sein. Fehler bei der Umsetzung des Notfallplans können somit weitreichende Folgen haben.

### Faktor Mensch

Selbst das ausgeklügeltste Datenschutzmanagementsystem bietet keinen absoluten Schutz vor Datenschutzverletzungen und häufig ist der Mensch die Schwachstelle, sei es aus Unwissen oder Unachtsamkeit. Wichtiger Teil der

Präventionsmassnahmen sind daher regelmässige Schulungen der Mitarbeitenden, um sie für Datenschutzthemen und damit zusammenhängende Risiken zu schulen.

### Kurzabriss weiterer Änderungen im rev. DSG

Das revidierte Gesetz führt neben der Meldepflicht für Datenschutzverletzungen weitere Pflichten und Instrumente ein, die europäische Unternehmen im Rahmen der Umsetzung der DSGVO-Pflichten bereits bestens kennen.

Eine wesentliche Verschärfung im revidierten DSG findet analog zur DSGVO im Bereich der Dokumentationspflichten statt. So gilt für Unternehmen grundsätzlich eine Pflicht, ein Bearbeitungsverzeichnis über Datenbearbeitungsaktivitäten zu führen. Von der Pflicht zur Führung eines Bearbeitungsverzeichnisses sind Unternehmen mit weniger als 250 Mitarbeitenden ausgenommen, sofern deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeitsrechte betroffener Personen mit sich bringt. Das Verzeichnis ist primär ein internes Dokument, mit welchem die bestehenden Datenprozesse dokumentiert werden. Formvorschriften macht das Gesetz keine, legt jedoch die Mindestangaben fest. Diese sind:

- Identität des Verantwortlichen
- Bearbeitungszweck
- Kategorien betroffener Personen und Personendaten
- Kategorien der Empfängerinnen
- Definition eines Qualitätsmanagementprozesses inkl.
- Aufbewahrungsdauer der Personendaten
- Massnahmen zur Gewährleistung der Datensicherheit
- Angaben des Empfängerstaates und Garantien

Des Weiteren untersteht das Outsourcing von Bearbeitungsaktivitäten im neuen

Recht strengeren Anforderungen als bisher. Da praktisch alle Unternehmen einen Teil der Verarbeitung personenbezogener Daten an einen Auftragsbearbeiter, bspw. an IT-Dienstleister, delegieren, sollten Verträge mit Auftragsbearbeitern einer Überprüfung unterzogen werden. Die wichtigste Neuerung in diesem Zusammenhang dürfte die Genehmigungspflicht für den Einsatz von Unterauftragsbearbeitern sein.

Obwohl Datenschutzerklärungen bereits jetzt als Instrument zur Information der betroffenen Personen weit verbreitet sind, besteht unter dem geltenden Schweizer Datenschutzrecht keine Pflicht zur Verwendung einer Datenschutzerklärung. Im revidierten Recht hingegen wird eine erweiterte Informationspflicht eingeführt und Unternehmen dazu verpflichtet, proaktiv Mindestangaben zu den von ihnen erhobenen und bearbeiteten Personendaten zu machen. Hinsichtlich der Form der Datenschutzerklärung macht das revidierte DSG keine Vorschriften. Die Information muss im Zeitpunkt der Erhebung der Daten erfolgen, d.h., es ist anstelle einer umfassenden Datenschutzerklärung auch möglich, Datensubjekte für jede spezifische Erhebung separat zu informieren.

Das revidierte Recht führt auch ein neues Verfügungs- und Bussenregime ein. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) erhält die Möglichkeit, Verfügungen hinsichtlich konkreter Datenbearbeitungsvorgänge gegenüber Unternehmen zu erlassen und die kantonalen Strafbehörden können neu eine Busse für bestimmte vorsätzliche Verletzungen des revidierten DSG bis zu einer Höhe von CHF 250'000 aussprechen. Allesamt Gründe für Unternehmen diesseits und jenseits der Schweizer Grenze, sich möglichst rasch mit den Änderungen vertraut zu machen und Massnahmen zu prüfen, so dass sie per Mitte 2022 auf Kurs sind, wenn das neue Recht in Kraft tritt.



# Handelskammerjournal

Ein Service der Handelskammer Deutschland Schweiz

[www.handelskammerjournal.ch](http://www.handelskammerjournal.ch)