epartners Rechtsanwälte AG
Puls 5 | Hardturmstrasse 11 | CH-8005 Zürich
T +41 43 268 8777 | F +41 43 268 8779
www.epartners.ch

epartners
Rechtsanwälte
Attorneys-at-Law

Marius Vischer und Mascha Santschi Kallay
August 2023

e:2.23

UMGANG MIT SICHERHEITSLECKS UNTER DEM REVIDIERTEN DSG

Kaum ein Tag vergeht, an welchem wir in den Zeitungen nicht über Cyber Angriffe lesen. Neu müssen solche Sicherheitsvorfälle dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gemeldet werden. Im Folgenden zeigen wir auf, wie sich Unternehmen darauf vorbereiten können und was im Fall der Fälle vorzukehren ist. Unser Beitrag beschränkt sich dabei nicht nur auf die rein juristischen Themen, sondern berücksichtigt auch unsere Erfahrungen aus der Praxis und den kommunikativen Umgang mit Sicherheitsvorfällen.

Gewährleistung der Datensicherheit

Am 1. September 2023 tritt in der Schweiz das revidierte Datenschutzgesetz (revDSG) in Kraft, welches in weiten Teilen eine Angleichung an die Rechtslage in der Europäischen Union (DSGVO) zur Folge hat. Damit rückt das Thema Datenschutz auch in der Schweiz vermehrt in den Fokus. Die Revision hat im Wesentlichen einen Ausbau der Governance von Unternehmen zur Folge (z.B. Datenschutzerklärung, Bearbeitungsverzeichnisse, Datenschutzfolgeabschätzungen). Weitere Ausführungen zur Revision finden Sie im epartners Fokus e:1.22.

In Bezug auf die Datensicherheit müssen Unternehmen wie bisher durch geeignete technische und organisatorische Massnahmen (sog. TOMs) eine dem Risiko angemessene Datensicherheit gewährleisten. Typische Massnahmen zur Erreichung angemessener Datensicherheit sind z.B. Zugriffs- und Zugangsbeschränkungen, Datenverschlüsselung, Backups, Bewachung, Alarmanlagen, aber auch Reglemente, Weisungen und Schulungen.

Zwar bleiben die Anforderungen in Bezug auf die Datensicherheit unter dem revDSG grundsätzlich unverändert. Was sich jedoch stetig verschärft, ist die Bedrohungslage. Insbesondere Cyber Angriffe nahmen in den letzten Jahren stark zu. Eine Auseinandersetzung mit der Thematik Datensicherheit, allenfalls unter Hinzuziehung von externen Spezialisten, gewinnt vor diesem Hintergrund an Aktualität.

Meldepflicht bei Datensicherheitsverletzungen

Mit dem Inkrafttreten des revDSG im September 2023 müssen Sicherheitsvorfälle, d.h. Verletzungen der Datensicherheit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet werden, wenn sie zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen.

Gemäss Gesetz ist ein solcher bisweilen auch als *Data Breach* bezeichneter Sicherheitsvorfall "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" (Art. 5 lit. h revDSG).

Beispiele für Data Breaches sind:

- Cyber Angriffe, die einen Zugriff auf Daten durch die Angreifenden oder einen Verlust des Zugriffs auf Daten für das Opfer des Angriffs zur Folge haben
- Verlust oder Diebstahl von Datenträgern (z.B. USB-Sticks, Tablets, Laptops)
- Versand von Bankauszügen oder Lohnausweisen an falsche Adressaten
- Versand von E-Mails mit heiklen Daten an einen falschen Abnehmerkreis

Die Meldung an den EDÖB hat durch den für die Datenbearbeitung Verantwortlichen (*Controller*) zu erfolgen. Auftragsbearbeiter (*Processor*) müssen deshalb Verletzungen der Datensicherheit nicht direkt dem EDÖB melden, sondern dem Controller – und zwar so rasch als möglich. Auftragsdatenbearbeitungsverträge sehen üblicherweise Fristen vor, innert welcher eine solche Meldung des Processors an den Controller zu erfolgen hat (i.d.R. zwischen 24 und 48 Stunden). Der Controller hat dann zu prüfen, ob er eine Meldung an den EDÖB machen muss.

Weiter sind auch die vom Vorfall betroffenen Personen zu informieren, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt. Dies ist zum Beispiel der Fall, wenn eine Änderung des Passwortes oder die Sperrung der Kreditkarte das Schadensrisiko der betroffenen Personen verringern könnte. Von der Informierung der einzelnen Betroffenen kann abgesehen werden, wenn an ihrer Stelle eine öffentliche Bekanntmachung erfolgt, etwa durch eine Medienmitteilung, und so die Information in vergleichbarer Weise sichergestellt ist.

Nach Eingang der Meldung prüft der EDÖB, ob die bereits getroffenen Massnahmen ausreichen, um den Vorfall zu behandeln und um zukünftige ähnliche Vorfälle zu verhindern. Mit einer Stellungnahme hält er fest, welche Massnahmen allenfalls noch vorzunehmen sind. Auch kann er meldende Unternehmen beraten. In einem Strafverfahren darf die EDÖB-Meldung gegen die meldepflichtige Person nur dann verwendet werden, wenn diese damit einverstanden ist.

Neben der Meldung an den EDÖB sollten Strafanzeige und eine Meldung an das Nationale Zentrum für Cybersicherheit (NCSC) gemacht werden. Allenfalls bestehen darüber hinaus vertragliche Verpflichtungen zur Informierung von Vertragspartnern oder, je nach Branchenzugehörigkeit oder Ausrichtung eines Unternehmens, auch Meldepflichten an weitere inländische oder ausländische Behörden (z.B. FINMA, ausländische Datenschutzbehörden). Es gehört zur *Due Diligence* eines Unternehmens zu wissen, an welche Behörde im Ernstfall eine Meldung zu erfolgen hat. Dabei ist zu beachten, dass diese Meldepflichten andere Fristen als das revDSG für die Meldung vorsehen können.

Data Breach Management

Die Abwägung, ob im Einzelfall eine Verletzung zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, muss das Unternehmen selbst vornehmen. Erfolgt eine Meldung zu Unrecht nicht, drohen keine Bussen. Hingegen kann es im Extremfall zu einer Busse kommen, wenn die Mindestanforderungen an die Datensicherheit nicht eingehalten werden.

Diese Abwägung wird Unternehmen regelmässig schwerfallen, zumal die Entscheidungsträger im Falle eines Cyber Angriffs unter enormem Druck stehen dürften, etwa weil aufgrund des Vorfalls keine Zugriffsmöglichkeit auf die benötigten Daten besteht, sie mit Erpressungsversuchen konfrontiert sind, keine Erfahrungswerte vorliegen und die Zeit drängt. Im Unterschied zur Regelung in der EU besteht zwar keine Frist, innert welcher

die Meldung zu erfolgen hat (dort 72 Stunden). Das Gesetz sieht jedoch vor, dass eine solche "so rasch als möglich" erfolgen muss (Art. 24 Abs. 1 revDSG). Die erwähnten 72 Stunden werden sich wohl auch hier als Richtwert etablieren. Oftmals wird deshalb eine Meldung erfolgen müssen, bevor die Sachverhaltsanalyse abgeschlossen ist. Die vorläufige Meldung kann dann zu einem späteren Zeitpunkt ergänzt werden. Neben der Ergreifung der notwendigen Sofortmassnahmen muss deshalb der Abklärung der Meldeplicht höchste Priorität zukommen.

Wir empfehlen Unternehmen, interne Prozesse zu erarbeiten, wie im Ernstfall vorzugehen ist. Sind die Prozesse im Unternehmen klar, mindert dies den Druck auf sämtliche Involvierten und sensibilisiert die Mitarbeitenden. Eine Auseinandersetzung mit u.a. folgenden organisatorischen Fragen erscheint uns dabei wichtig, wobei die Antworten in Form eines Konzepts im Krisenfall sofort auffindbar sein sollten:

- Wer wird intern über einen Vorfall informiert und auf welchem Kommunikationsweg?
- Wie wird die externe Erreichbarkeit sichergestellt und durch welche Personen, d.h. bezüglich Kunden, Lieferanten, Partnern oder Medien? Gibt es eine Notfallnummer, die 24/7 erreicht werden kann?
- Welchen Support holt man sich extern (z.B. IT-Security, IT-Forensiker, Anwalt, Kommunikationsspezialist) und welche Mitarbeitenden decken die Schnittstellen ab?
- Wer ist für die Sachverhaltsanalyse zuständig?
- Wer entscheidet, ob eine Meldung gemacht wird und wer tritt gegenüber dem EDÖB als Kontaktperson auf?
- Liegen Meldepflichten an weitere Behörden vor (z.B. FINMA, ausländische Behörden)?

Sachverhaltsanalyse

Verletzungen der Datensicherheit sind zu dokumentieren, z.B. in der Form einer Aktennotiz. Der Vorfall, seine Auswirkungen und die ergriffenen Massnahmen sind zu beschreiben. Die Dokumentation muss mindestens zwei Jahre aufbewahrt werden. Wir empfehlen, dass sich die Dokumentation auch zur Frage äussert, ob der Vorfall dem EDÖB gemeldet wurde. Obwohl nicht Pflicht, sollte eine Dokumentation auch dann erstellt werden, wenn keine Meldung an den EDÖB erfolgt. Damit kann belegt werden, dass man sich seriös mit dem Vorfall auseinandergesetzt hat. Auch hilft dies bei der Identifizierung von Massnahmen zur Verbesserung des Data Breach Konzeptes.

Die Dokumentation umfasst eine vollständige Sachverhaltsanalyse. Diese beinhaltet folgende Punkte:

- Zeitpunkt und Dauer des Vorfalls, Zeitpunkt der Feststellung
- Wer intern Meldung erstattet hat und wer informiert worden ist (intern/extern)
- Ob bereits Informationen an die Öffentlichkeit gelangt sind oder ob damit zu rechnen ist
- Art der Verletzung (Vernichtung/Löschung, Verlust, Veränderung, Bekanntgabe an Unbefugte)
- Auslöser des Vorfalls
- Betroffene Systeme, Personen (Mitarbeitende, Kunden, Lieferanten), Daten (E-Mail-Adressen, Passwörter etc.) und Umfang des Vorfalls (Anzahl betroffener Daten und Personen)
- Welche Sofortmassnahmen getroffen worden sind
- Wahrscheinliche Folgen und Risiken für die betroffenen Personen

Eine klare Sachverhaltsanalyse erleichtert die Erstellung der Meldung an die Behörde(n), zumal der Inhalt weitgehend identisch sein dürfte. Was die Meldung an den EDÖB betrifft, so wird hierfür auf seiner Website ein Formular zur Verfügung stehen. Auch wenn der EDÖB eine Meldung mittels seines Formulars bevorzugen wird, ist dieses nicht zwingend

zu verwenden. Bestehen Meldepflichten an verschiedene Behörden, ist eine Meldung mittels einer Stellungnahme, die sich zu den erforderlichen Themen äussert, oftmals zu bevorzugen.

Kommunikation

Auf den ersten Blick bestehen bezüglich der Kommunikation bei Datensicherheitsvorfällen einige Unsicherheiten, da die gesetzlichen Bestimmungen dem Unternehmen nicht jederzeit klar vorgeben, ob – und falls ja, gegenüber wem, auf welche Weise und zu welchem Zeitpunkt – eine externe Informierung erfolgen muss. Hingegen ermöglicht diese Ausgangslage den Entscheidungsträgern, im Krisenfall auch mediale, kommunikative, psychologische und unternehmensspezifische Faktoren in die Entscheide miteinzubeziehen. Solche Überlegungen helfen beispielsweise bei der Frage, wann eine Informierung der von einem Vorfall betroffenen Person angebracht ist, auf welche Weise eine Meldung an die Vertragspartner (Kunden, Geschäftspartner etc.) erfolgen soll oder ob der EDÖB miteinzubeziehen ist.

So kann es etwa sinnvoll sein, möglichst offen und transparent mit dem Vorfall umzugehen, um den Goodwill und das Vertrauen von Kunden und Geschäftspartnern nicht zusätzlich zu gefährden – auch wenn das Gesetz eine Informierung nicht verlangt. In diesem Zusammenhang ist interessant, dass das Gesetz eine Kommunikation nicht bereits vorsieht, wenn das Risiko einer Sicherheitsverletzung besteht, sondern erst dann, wenn eine solche vorliegt, sei es durch den Verlust, die Löschung, Vernichtung, Veränderung, Offenlegung oder Zugänglichmachung von Daten. Je nach den konkreten Umständen sollte eine Informierung jedoch auch bereits in einem früheren Stadium erwogen werden.

Es ist sodann möglich, dass die Information aus bestimmten Gründen nicht direkt an die oder an sämtliche vom Vorfall betroffenen Personen erfolgen kann und man via Medienmitteilung einen grösstmöglichen Adressatenkreis erreichen will. Diesfalls muss rasch eine Medienmitteilung erstellt werden, die formal professionell gestaltet, inhaltlich zutreffend und rechtlich unverfänglich formuliert ist. Das kann einem Kunststück gleichen, zumal der Sachverhalt zu diesem Zeitpunkt kaum je bereits abschliessend geklärt sein dürfte, wobei aber auch über diesen Umstand zu informieren ist.

Im Weiteren muss regelmässig das latente Risiko in Betracht gezogen werden, dass die Medien oder eine gewisse Öffentlichkeit jederzeit auch auf inoffiziellem Weg von einem Datensicherheitsvorfall erfahren könnten, allenfalls auch, bevor das Unternehmen selber den Entscheid bezüglich der Kommunikation getroffen oder diese aufgegleist hat. Drohen Erpresser mit der Veröffentlichung von Daten im Darknet, ist damit zu rechnen, dass die Daten nach Ablauf der gesetzten Frist tatsächlich veröffentlich und damit der (Medien-) Öffentlichkeit zugänglich gemacht werden.

Eine unterlassene oder zu späte Informierung kann unter Umständen ein zivilrechtliches Haftungsrisiko nach sich ziehen, wenn der betroffenen Person dadurch ein Schaden entstanden ist. Daran vermögen auch die im Gesetz fehlenden Sanktionen in Bezug auf Datensicherheitsvorfälle nichts zu ändern, da diese keinen Einfluss auf das Zivilrecht zeitigen.

Datensicherheitsvorfälle können einen Imageschaden bewirken. Häufig wird unterschätzt, dass das Verhalten in der Krisensituation mindestens so relevant ist wie die Tatsache, dass es überhaupt zu einem Datensicherheitsvorfall gekommen ist. Es empfiehlt sich deshalb auch vor diesem Hintergrund, für den Fall eines Cyber Angriffs ein Konzept zu erarbeiten, das im Ernstfall rasch zur Hand ist und die wichtigsten Vorgehensweisen sowie die zu involvierenden und informierenden Personen nennt.

Fazit

Unternehmen sind gut beraten, sich rechtzeitig damit auseinanderzusetzen, wie im Falle eines Data Breaches vorgegangen wird. Ein auf das spezifische Unternehmen zugeschnittener Prozess und die interne Sensibilisierung können im Notfall grossen Mehrwert bieten.

Es empfiehlt sich, bei einem Datensicherheitsvorfall nicht nur auf einen versierten Anwalt, sondern auch auf eine auf Rechtskommunikation spezialisierte Expertin zurückzugreifen. Dies ist deshalb wichtig, weil sich die juristisch-forensische und die kommunikativ-mediale Arbeitsweise einerseits stark voneinander unterscheiden, andererseits in Kombination sogar ein ideal ergänztes Vorgehen während einer Krise ermöglichen. Im besten Fall kennen sich der zuständige Anwalt und die beauftragte Kommunikationsexpertin bereits aus früherer Zusammenarbeit und funktionieren auch unter Zeitdruck als eingespieltes Team. Hier bietet epartners Rechtsanwälte juristischen und medialen Support aus einer Hand an.

Gerne unterstützen wir Sie bei der Erarbeitung der notwendigen Grundlagen, sowohl im Recht als auch in der Kommunikation.

epartners Rechtsanwälte AG