TALOS

Publication

Verfahren bei Verletzungen des Schutzes personenbezogener Daten

Handlungsempfehlungen für Finanzdienstleister

von Christian Scholten und Thomas Eustorgi

In unserer digitalisierten Welt werden Datenpannen, also Verstösse gegen den Datenschutz bei denen personenbezogene Daten Unberechtigten bekannt werden, immer häufiger entdeckt und an die entsprechenden Datenschutzbehörden gemeldet.[1] Die Folgen einer solchen Datenpanne können schwerwiegend sein und ernsthafte betriebliche, finanzielle und reputationsbezogenen Schäden verursachen. Besonders anfällig sind dabei Finanzdienstleister, da sie eine grosse Menge sensibler Daten bearbeiten und gleichzeitig einer verstärkten Kontrolle durch die Aufsichtsbehörden unterstehen.

Aus operativer Sicht benötigen Finanzdienstleister ein Verfahren, um bei Verletzungen des Schutzes personenbezogener Daten rasch reagieren zu können und die Aufsichtsbehörden, betroffene Kunden sowie weitere Anspruchsgruppen zeitnah zu informieren. Die erforderlichen Verfahren und Massnahmen, welche mitunter die Offenlegung der betroffenen Daten beinhaltet, bergen erhebliche betriebliche und finanzielle Risiken. Daher sind Organisationen gut beraten, auf die Erfahrung professioneller Dienstleister für Rechtsberatung und für die Planung und Ausführung der erforderlichen Verfahren und Massnahmen zurückzugreifen.

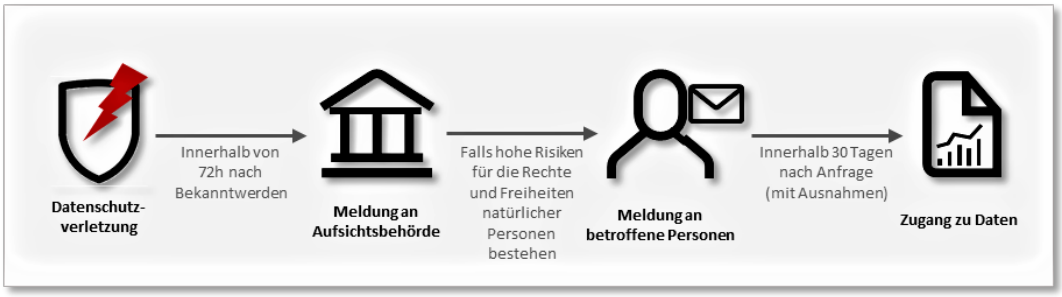
Fussnote:
1 Einige EU-Datenschutzbehörden erhalten pro Jahr bis zu 70 Meldungen pro 100.000 Einwohner (GDPR today, www.gdprtoday.org/gdpr-in-numbers-4)

TALOS

Publication

Verletzung des Schutzes personenbezogener Daten und DSGVO

Die Datenschutz-Grundverordnung der EU (DSGVO) definiert die Rechte *betroffener Personen*[2] – beispielsweise Kunden oder Mitarbeiter – im Falle einer Datenschutzverletzung bei welcher personenbezogene Daten Unberechtigten bekannt werden. Gemäss DSGVO Art. 32 muss der *Auftragsverarbeiter*, z.B. eine Bank, jede Verletzung innerhalb von 72 Stunden nach Bekanntwerden der Aufsichtsbehörde melden. Der *Auftragsverarbeiter* ist des Weiteren gesetzlich verpflichtet die *betroffenen Personen* zu benachrichtigen sofern die Verletzung zu einem hohen Risiko für die *Rechte und Freiheiten*[3] natürlicher Personen führen könnte (DSGVO Art. 33). Falls dies zutrifft, so hat der *Auftragsverarbeiter* jede *betroffene Person* einzeln und vorzugsweise schriftlich zu benachrichtigen.[4] Darüber hinaus ist der *Auftragsverarbeiter* nach DSGVO Art. 15 verpflichtet, Zugang zu personenbezogenen Daten zu gewähren und eine Anlaufstelle (Helpdesk) einzurichten. Unter bestimmten Umständen muss den *betroffenen Personen* auch eine Kopie von Dokumenten, wie z.B. die Kopie einer E-Mail ausgehändigt werden.[5]



Fussnoten:
2 Im Englischen spricht man von data subject («Datensubjekten»)

3 Das Risiko für die Rechte und Freiheiten beinhaltet z.B. das Risiko von Diskriminierung, Identitäts-diebstahl, finanziellem Verlust oder Reputations-schäden (vgl. EU-DSGVO, Erwägungsgrund 75)

4 Falls dies zu einem unverhältnismässigen Aufwand führen würde, kann die Verletzung öffentlich bekanntgeben werden.

Abbildung 1: Meldeverfahren gemäss DSGVO

5 Da sich der weit gefasste Wortlaut von DSGVO Art. 15 darüber ausschweigt, was der Verantwortliche in der Praxis genau zur Verfügung stellen muss, gehen die Meinungen über die Reichweite des Anspruchs auf Auskunftserteilung und Aushändigung einer Kopie entsprechend weit auseinander.

Verfahren bei Verletzung des Schutzes personenbezogener Daten

Das von uns empfohlene Verfahren im Falle einer Verletzung des Schutzes personenbezogener Daten kann in sechs Schritte unterteilt werden (Abb. 2).

Als Erstes (Schritt 1) sind technische Massnahmen zur Erkennung eines Verstosses, dessen Eindämmung und Beseitigung sowie zur Datenwiederherstellung zu ergreifen. Dazu muss man die Verletzung analysieren, die betroffenen Daten identifizieren und massgeschneiderte Sofortmassnahmen zur Prävention weiterer Verstösse implementieren.

Sehr bald stellt sich für das Unternehmen die Frage, wie mit der Datenschutzverletzung umzugehen ist. Hierzu ist eine strategische Planung der nächsten Schritte notwendig (Schritt 2). Eine Datenschutzverletzung ist der Aufsichtsbehörde unverzüglich innerhalb von 72 Stunden nach Bekanntwerden des Verstosses zu melden. Vom Zeitpunkt der Meldung lohnt es sich eine effiziente Kommunikation mit den Behörden zu pflegen, da eine einmalige Meldung selten ausreichen wird.

Ein rechtliches Gutachten sollte Auskunft darüber geben, ob und wie die *betroffenen Personen* benachrichtigt werden müssen und in welchem Umfang sie ein Recht auf Zugang zu ihren Daten haben. Das rechtliche Guthaben sollte auch pragmatische Fragen beantworten,

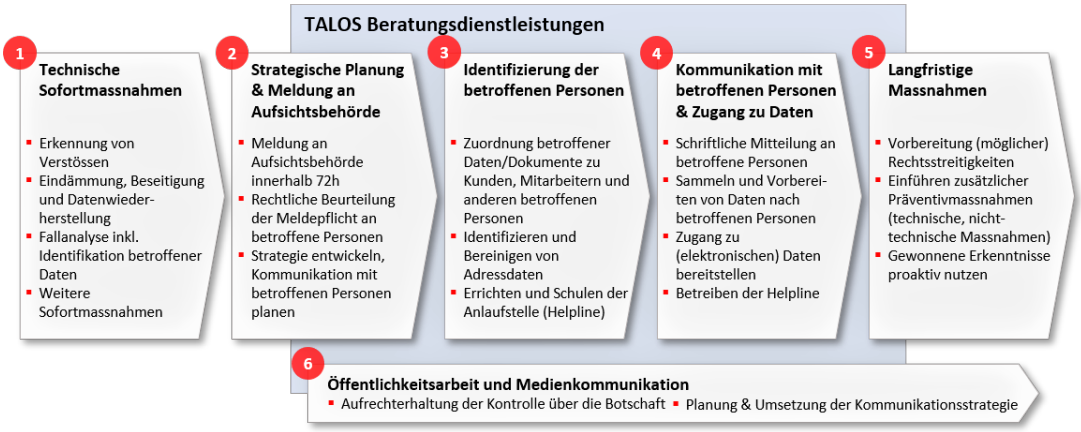


Abbildung 2:
Das Verfahren bei Verletzung des Schutzes personenbezogener Daten in 6 Schritten

Fussnote:
6 Der Zeitraum kann je nach Komplexität und Anzahl der Anfragen um weitere 60 Tage erweitert werden (DSGVO Art. 12).

wie beispielsweise, welche Rolleninhaber eines Kontos kontaktiert werden müssen (bei einer Bank) oder ob die *betroffenen Personen* per E-Mail kontaktiert werden können.

Ist das weitere Vorgehen in den Grundzügen definiert, müssen in Schritt 3 die *betroffenen Personen* identifiziert werden. In der Praxis wird oftmals eine Kombination aus automatisierter Datenanalyse und manueller Überprüfungen der Ergebnisse angewendet. Als Beispiel nehmen wir an, dass eine Bank die betroffenen Daten nach Kontonummern durchsucht. Die automatisch generierten Ergebnisse müssen danach einer manuellen falsch-positiv Überprüfung unterzogen werden, um sicherzustellen, dass die Nummern einem Konto und nicht einer Telefonnummer o.ä. zuzuordnen sind.

Sobald die *betroffenen Personen* identifiziert sind, müssen Adressdaten abgefragt, bereinigt und eventuell sogar manuell ergänzt werden. Diese Adressbereinigung ist insbesondere für ehemalige Kunden relevant oder in Fällen wo die Benachrichtigungsadresse von der regulären Postanschrift abweicht.

Als letzte Aktivität im Schritt 3 muss eine Anlaufstelle für Rückfragen eingerichtet werden. Nur diese Anlaufstelle sollte befugt sein mit *betroffenen Personen* über Angelegenheiten im Zusammenhang mit der Datenschutzverletzung zu kommunizieren. Dabei hat sich die Stelle an vorher definierte Leitlinien zu halten, um Inkonsistenzen in der Kommunikation zu vermeiden.

In Schritt 4 folgt nun die Benachrichtigung aller *betroffenen Personen*. Um Rückfragen besser zu handhaben, ist die Benachrichtigung gestaffelt zu senden.

Ein gewisser Anteil der *betroffenen Personen* wird in der Folge Zugang zu den betroffenen Daten verlangen. Das Unternehmen muss folglich bereits frühzeitig Vorbereitungen treffen, um innerhalb einer angemessenen Frist, in der Praxis innerhalb von 30 Tagen[6], Zugang zu den Daten zu gewähren. Dabei müssen Daten von Drittpersonen vor der Offenlegung geschützt werden. Auf dem Markt gibt es dafür zwar Softwarelösungen, welche Daten von Drittpersonen erkennt und abdeckt, trotzdem wird ein gewisses Mass an manueller Qualitätssicherung weiterhin notwendig sein.

Betroffenen Personen ist auf möglichst effiziente Weise Zugang zu ihren Daten zu gewähren. Dafür eignet sich in der Regel ein elektronisches Format. Die Daten können zum Beispiel in einen virtuellen Datenraum hochgeladen werden worauf *betroffene Personen* mit einem individuellen Benutzerprofil zugreifen können.

In Schritt 4 ist es wichtig, dass alle Aktivitäten, jeder Kundenkontakt, jede Anfrage oder jede Bereitstellung von Zugangsdaten erfasst wird. Die Abläufe sollten idealerweise in einem Workflow-Management-Tool abgebildet werden.

In Schritt 5 müssen schliesslich die Vorbereitungen für die langfristigen Massnahmen geplant werden. Dazu gehört die Vorbereitung auf mögliche Rechtsstreitigkeiten oder die Umsetzung zusätzlicher Abwehrmassnahmen, um das Risiko weitere Datenschutzverletzungen zu reduzieren.

Durch eine wirksame Öffentlichkeitsarbeit und Medienkommunikation (Schritt 6) gilt es vom ersten Tag an weitere Reputationsschäden zu verhindern. Das Unternehmen darf die Kontrolle über die Informationen und die Diskussionen in der Öffentlichkeit nicht aus der Hand geben.

Anwendungsbeispiel

Die Herausforderung

Unser Kunde erlitt eine Datenpanne in der Schweiz und einem EU-Land, was dazu führte, dass personenbezogene Daten von Kunden und Mitarbeitern für eine ausländische Behörde zugänglich waren. Der Kunde war verpflichtet die betroffenen Personen über den Datenschutzverstoss zu informieren. Mehrere betroffene Personen in der Schweiz und in der EU haben daraufhin Zugang zu Daten und Dokumenten verlangt.

Unser Beitrag

Für unseren Kunden haben wir den End-zu-End-Benachrichtigungs- und Offenlegungsprozess konzipiert und implementiert. Unsere Berater unterstützten bei der Identifizierung betroffener Personen, bei der Benachrichtigung von Kunden und Mitarbeiter sowie beim Betrieb eines Helpdesks. TALOS definierte die Rolle von Kundenteams, entwickelte Richtlinien und Arbeitsanweisungen und implementierte Tools zur Überwachung des Status jeder einzelnen Anfrage. Temporäre Ressourcen von TALOS unterstützten zudem bei der Abdeckung von Daten Dritter. Für den Kunden koordinierte TALOS fast alle mit dem Datenleck verbunden Aktivitäten angefangen vom Projektmanagement bis hin zur Identifikation der betroffenen Personen und der Qualitätssicherung vor der Offenlegung relevanter Daten und Dokumente.

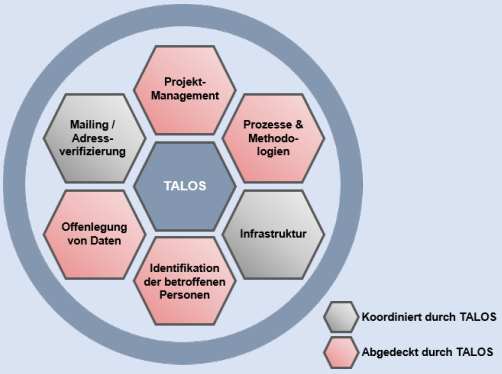


Abbildung 3:
Von TALOS abgedeckte/ koordinierte Dienstleistungen in einem konkreten Anwendungsfall

Der Kundenutzen

Der Kunde konnte sich auf uns als eine zentralisierte Funktion verlassen, welche sowohl mit internen Anspruchsgruppen, wie auch mit spezialisierten Anbietern zusammenzuarbeitet und so alle Verfahrensschritte von der strategischen Planung bis zur Offenlegung der betroffenen Daten entweder selbst oder in Kooperation mit anderen Dienstleistern und internen Stellen abdecken konnte.

Schlusswort

Eine Verletzung des Schutzes personenbezogener Daten löst eine Reihe verbindlicher operativer Verfahren aus. Darunter fallen die Meldung an die Aufsichtsbehörden, die Identifizierung betroffener Daten und Personen, die Benachrichtigung und Kommunikation mit Kunden und Mitarbeitern, sowie die Offenlegung relevanter Daten. Die Steuerung dieser Verfahren erfordert einen interdisziplinären Ansatz, das Wissen spezialisierter Anbieter, juristisches Know-how und Projektmanagement-Fähigkeiten. Wenn diese operativen Verfahren nicht ordnungsgemäss geplant und ausgeführt werden, führen Fehler und andere Ineffizienzen rasch zu weiteren finanziellen Verlusten und Reputationsschäden. Unternehmen sind daher gut beraten auf das Wissen und die Erfahrung professioneller Anbieter zurückzugreifen, die in der Lage sind, die interdisziplinären Aspekte einer Verletzung des Schutzes personenbezogener Daten zu steuern und zu koordinieren.

TALOS

Publication

Who we are

TALOS definiert neue Standards in der Management Beratung. Als spezialisierte Boutique Beratung mit Schweizer Wurzeln und Büwros in Zürich und Luxemburg beraten wir Kunden aus der Europäischen Finanzindustrie.

TALOS wurde 2008 von erfahrenen Management Beratern gegründet und ist seither zu einem etablierten Beratungsunternehmen für Finanzunternehmen gewachsen.

Als Experten für regulatorische Transformationslösungen decken wir die gesamte Bandbreite möglicher Fragestellungen ab, von der Analyse über die Strategie bis hin zur Umsetzung.

Zürich
TALOS Management Consultants
Bleicherweg 45
CH-8002 Zürich
Tel. +41 44 380 14 40

Luxembourg
TALOS Management Consultants
6, Rives de Clausen
L-2165 Luxembourg
Tel. +352 26 20 23 54

www.talos-consultants.com
www.shapenewstandards.com

Your Contact

Christian ist Partner bei TALOS und arbeitete früher als interner Berater für einen deutschen Logistikkonzern und ist seit 2007 als Unternehmensberater (Accenture, TALOS) tätig.

Christian Scholten
Partner
christian.scholten@talos-consultants.ch

Thomas ist Manager und kam 2016 zu TALOS. Er verfügt über mehr als 8 Jahre Erfahrung in der Finanzdienstleistungsbranche mit einer weltweiten Karriere in der Schweiz, den USA, Spanien und Südkorea. Thomas bringt funktionale Expertise und Projekterfahrung in den Bereichen Compliance, Outsourcing und Finanzmanagement ein.

Thomas Eustorgi
Manager
thomas.eustorgi@talos-consultants.ch