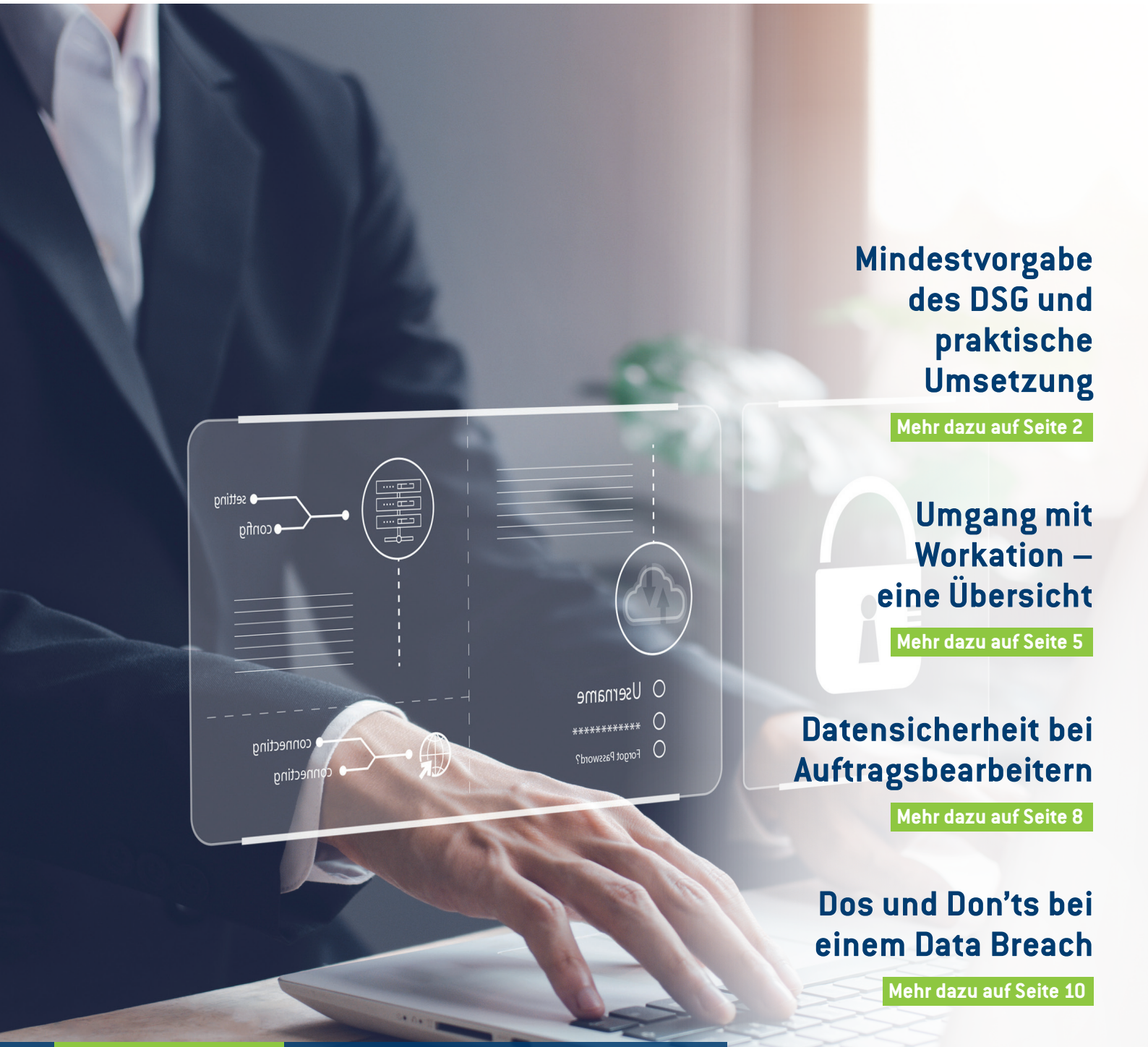
AUSGABE 04
APRIL 2025

binder rechtsanwälte

WEKA

DATENSCHUTZ

FÜR SCHWEIZER UNTERNEHMEN UND INSTITUTIONEN



In dieser Ausgabe

Datensicherheit

Datensicherheit ein Top-Down-Thema

In den meisten Umfragen zu den Prioritäten von Geschäftsführern für das Jahr 2025 rangiert das Thema «Datensicherheit» bzw. «Cybersecurity» auf den vordersten Plätzen. Der Hauptgrund dafür veranschaulicht ein Zitat von Serene Davis (Global Head of Cyber, QBE Insurance) «A breach alone is not a disaster, but mishandling it is.». Diese Aussage enthält zwei zentrale Punkte, nämlich, dass eine Verletzung der Datensicherheit jeden zu jederzeit treffen kann und, dass der Umgang mit einem solchen Vorfall zentral ist.

Gerade weil das Risiko hoch ist, dass ein Unternehmen von einem Datensicherheitsvorfall betroffen sein wird, ist die Vorbereitung darauf zentral, den die Folgen können gravierend sein. Das tönt auf den ersten Blick trivial, stellt Unternehmen aber vor grosse Herausforderungen. Wesentlich dabei ist, dass die Geschäftsleitung das Thema priorisiert und die Wichtigkeit hervorhebt. In der Praxis hat sich gezeigt, dass die Reaktion auf einen Datensicherheitsvorfall von der Geschäftsleitung und den ausgewählten Schlüsselfunktionen trainiert werden sollte. Aus datenschutzrechtlicher Sicht kann zudem eine Meldepflicht bei der zuständigen Behörde bestehen. Dazu hat der EDÖB kürzlich einen Leitfaden herausgegeben, der die rechtlichen Voraussetzungen behandelt.

Viel Spass bei der Lektüre

Marco S. Meier, RA, MLaw, CIPP/E
Herausgeber

Mindestvorgaben des DSG und praktische Umsetzung

Technologische Fortschritte eröffnen neue Chancen, bringen jedoch auch Herausforderungen und Risiken mit sich. Das Datenschutzgesetz **(DSG)** trägt dem Rechnung, indem es klare Anforderungen an die Datensicherheit stellt. Unternehmen sind verpflichtet, technische und organisatorische Massnahmen **(TOMs)** zu implementieren, um den Schutz von Personendaten sicherzustellen. Viele KMU stehen hier aber vor der Herausforderung, festzustellen, welche TOMs nun für ihr konkretes Geschäftsmodell im Sinne des Gesetzes nötig sind.

Von Dr. iur Lukas Lezzi

Datensicherheit

Gemäss Art. 8 DSG sind Verantwortliche und Auftragsbearbeiter verpflichtet, angemessene TOMs zu ergreifen, um die Datensicherheit zu gewährleisten. Der Verantwortliche hat zudem sicherzustellen, dass der von ihm beauftragte Auftragsbearbeiter die erforderlichen Anforderungen erfüllt und über die nötigen TOMs verfügt.

Mindestanforderungen an die Datensicherheit

Art. 1 Datenschutzverordnung **(DSV),** Art. 2 DSV und Art. 3 DSV bestimmen die Mindestanforderungen an die Datensicherheit. Die Mindestanforderungen agieren nicht als zwingende Massnahmen, sondern Kriterien, die zu berücksichtigen sind. Sie orientieren sich an den Grundsätzen der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit. Die Mindestanforderungen umfassen Folgendes:

- **Vertraulichkeit:**
  - Zugriffskontrolle: Personen dürfen nur auf Personendaten Zugriff haben, welche sie zur Erfüllung ihrer Aufgaben benötigen.
  - Zugangskontrolle: Nur berechtigte Personen dürfen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden.
  - Benutzerkontrolle: Unbefugte Personen dürfen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen können.
- **Verfügbarkeit und Integrität:**
  - Datenträgerkontrolle: Unberechtigte Personen dürfen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten.
  - Speicherkontrolle: Unberechtigte Personen dürfen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können.
  - Transportkontrolle: Unberechtigte Personen dürfen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten können.
  - Wiederherstellung: Die Verfügbarkeit der Personendaten und der Zugang zu ihnen muss bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.
  - Systemsicherheit: Betriebssysteme und Anwendungssoftware müssen stets auf dem neuesten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden.

  - Datenintegrität: Fehlfunktionen müssen gemeldet werden (Zuverlässigkeit), und gespeicherte Personendaten dürfen nicht durch Fehlfunktionen des Systems beschädigt werden können.

- **Nachvollziehbarkeit:**
  - Eingabekontrolle: Es muss überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden.
  - Bekanntgabekontrolle: Es muss überprüft werden können, wem Personendaten mithilfe von Einrichtungen zur Datenübertragung bekannt gegeben werden.
  - Erkennung und Beseitigung: Verletzungen der Datensicherheit müssen rasch erkannt werden, damit Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können.

Die gesetzlichen Mindestvorschriften geben hier erst einmal die grundsätzlichen Bereiche und Themen vor, welche anhand der Sensibilität der Personendaten, dem Stand der Technik und den Implementierungskosten konkretisiert werden müssen. Dies geschieht im Unternehmen durch die TOMs.

Technische und organisatorische Massnahmen («TOMs»)

Die TOMs müssen dem jeweiligen Risiko, welches die Datenbearbeitung für die betroffenen Personen mit sich bringt, angemessen sein. Dies bedeutet, dass ein risikobasierter Ansatz verfolgt werden muss. Dabei sind die Massnahmen nicht für alle Personendaten gleich auszugestalten, sondern müssen unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Datenbearbeitung an das jeweilige Risiko angepasst werden. Dabei sind die Prinzipien der Vertraulichkeit, Verfügbarkeit, Integrität und Nahvollziehbarkeit zu wahren. Grundsätzlich gilt: Je sensibler die Personendaten, desto umfassender und strenger müssen die Massnahmen sein.

Technische Massnahmen

Unter technischen Massnahmen sind alle Vorkehrungen zu verstehen, die entweder technische Mittel zum Erreichen eines Schutzziels nutzen, integraler Bestandteil eines technischen Systems sind oder dem physischen Schutz dienen (z. B. ein Passwortschutz, Virenscanner). Dies bedeutet, dass der Datenschutz bereits bei der Entwicklung eines neuen Projekts in Betracht gezogen werden soll. Dadurch soll sichergestellt werden, dass die Grundsätze des Datenschutzes durch Technik und Organisation eingehalten werden. Dementsprechend ist es nötig, die Datenbearbeitungsprozesse detailliert zu analysieren und ein Informationssicherheits- und Datenschutzkonzept auszuarbeiten. Folgende Punkte sollten als Standard implementiert werden:

- Zugriffskontrollen (z. B. Rollen- und Rechtekonzepte, Zwei-Faktor-Authentifizierung)
- Sicherung der Datenverfügbarkeit durch regelmässige Back-ups und Notfallpläne
- regelmässige Updates und Patches zur Behebung von Sicherheitslücken
- Schutzmechanismen wie Firewalls, VPN und Intrusion-Detection-Systeme
- Patch-Management (zur rechtzeitigen Einspeisung von Updates)
- geschützte Protokollierung
- Einsatz von Malware-/Virenscannern
- Zutrittsbeschränkungen wie etwa Personenvereinzelungsanlagen, Badge-Systeme, Irisscanner etc.

Basierend auf den Risiken, welche eine Datenbearbeitung für die betroffenen Personen hat, sollten die folgenden weiteren Massnahmen in Betracht gezogen werden:

- Anonymisierung und Pseudonymisierung
- Verschlüsselung von Personendaten (z. B. bei Übertragung oder auf Speicherebene)
- Fähigkeit zur raschen Wiederherstellung der Verfügbarkeit von und des Zugriffs auf Personendaten
- Implementierung von intelligenten Bearbeitungs- und Löschfunktionen

Hervorzuheben ist, dass die Implementierungskosten nicht als Grund herangezogen werden können, um keine oder ungenügende Massnahmen zu implementieren.

Obwohl oft der Begriff «Verschlüsselung» verwendet wird, ist die Verschlüsselung von Personendaten – also die Umwandlung von Klartextdaten in ein unlesbares Format – weder im Ruhezustand noch bei der Übertragung von Daten zwingend erforderlich. Eine ähnliche Wirkung, ohne dass das Dateiformat geändert werden muss, kann auch durch Anonymisierung (ein Verfahren, bei dem Daten so verändert werden, dass kein Rückschluss mehr auf die betroffene Person möglich ist, wobei der Personenbezug mit angemessenem Aufwand nicht wiederhergestellt werden kann) oder Tokenisierung (bei der sensible Daten durch eindeutige Identifikationssymbole ersetzt werden, die alle wesentlichen Informationen über die Daten enthalten) erzielt werden.

Organisatorische Massnahmen

Organisatorische Massnahmen zielen auf das Umfeld des Systems, insbesondere die Personen, die es nutzen, ab. Sie legen Zuständigkeiten, Aufgaben und Verantwortlichkeiten im Bereich der Informationssicherheit fest und definieren Verhaltensrichtlinien für Mitarbeitende (z. B. interne Richtlinien, Schulungen, Empfehlungen). Auf organisatorischer Ebene sollten folgende Punkte beachtet werden:

- «Need-to-know»-Prinzip implementieren
- die Datenbearbeitung dokumentieren
- Schulungen und Sensibilisierung der Mitarbeitenden in Datenschutzfragen

- strikte Clean Desk Policy
- Auftragsbearbeitungsverträge mit Dritten, die Zugang zu den Daten haben, abschliessen

Protokollierung

Art. 4 DSV verlangt in bestimmten Situationen die Protokollierung von Datenbearbeitungen. Ziel dieser Protokollierung ist es, sicherheitsrelevante Ereignisse zu erfassen, die entsprechenden Daten zu speichern und sie für eine spätere Auswertung bereitzustellen. Als Massnahme der Datensicherheit im weiteren Sinne dient die Protokollierung sowohl der präventiven Erkennung von Sicherheitsvorfällen als auch der nachträglichen Analyse von Datenschutzverletzungen. Sie trägt zur Erreichung des Schutzziels der Nachvollziehbarkeit bei (Art. 2 Abs. 1 lit. d DSV) und ergänzt die Massnahmen gemäss Art. 3 Abs. 3 DSV. In Fällen, in denen eine Protokollierung gesetzlich vorgeschrieben ist, zählt sie zu den Mindestanforderungen der Datensicherheit.

Verantwortliche und Auftragsbearbeiter sind zur Protokollierung verpflichtet, wenn besonders schützenswerte Personendaten in grossem Umfang und auf automatisierte Weise bearbeitet werden. Zusätzlich muss eine Protokollierung erfolgen, wenn ein Profiling mit hohem Risiko durchgeführt wird. Verantwortliche und Auftragsbearbeiter sind verpflichtet, mindestens die Vorgänge des Speicherns, Veränderns, Lesens, Bekanntgebens, Löschens und Vernichtens von Daten zu protokollieren. Die Protokolle sind während mindestens einem Jahr getrennt vom System, in welchem die Personendaten bearbeitet werden, aufzubewahren (vgl. Art. 4 Abs. 5 DSV).

Fazit

Unternehmen müssen angemessene TOMs implementieren, die sich an den spezifischen Risiken der Datenbearbeitung orientieren. Dabei sind Prinzipien wie Vertraulichkeit, Integrität und Nachvollziehbarkeit essenziell. Die Mindestanforderungen gemäss DSG und DSV bieten einen Rahmen für die Massnahmen, lassen jedoch genügend Spielraum für eine risikobasierte Anpassung. Unternehmen sollten den Datenschutz nicht als einmalige Massnahme, sondern als kontinuierlichen Prozess begreifen, der durch klare Verantwortlichkeiten, regelmässige Überprüfung und Anpassung an neue Entwicklungen getragen wird. Eine strategische und praxisnahe Umsetzung dieser Vorgaben ist entscheidend für eine nachhaltige Compliance.

Zusammenfassung

- Unternehmen sind verpflichtet, angemessene technische und organisatorische Massnahmen (TOMs) umzusetzen, um die Sicherheit von Personendaten zu gewährleisten. Die Mindestanforderungen des DSG und der DSV bieten einen Rahmen, müssen aber risikobasiert an das Unternehmen angepasst werden.
- Datenschutz erfordert eine Kombination aus technischen Sicherheitsvorkehrungen, organisatorischen Prozessen und Sensibilisierung der Mitarbeitenden. Besonders wichtige TOMs für KMU sind Zugriffskontrollen, Verschlüsselung, regelmässige Back-ups, Schulungen und Sicherheitsupdates.
- Datenschutz ist ein kontinuierlicher Prozess und keine einmalige Massnahme. Unternehmen müssen ihre Sicherheitsvorkehrungen regelmässig überprüfen, an neue Bedrohungen anpassen und eine nachhaltige Compliance-Strategie verfolgen.

TOP 10 TOMS

- Need-to-know-Prinzip
- Einsatz von starken Passwörtern, Zwei-Faktor-Authentifizierung (2FA) und rollenbasierte Berechtigungen
- automatische Back-ups auf externen, sicheren Speichermedien oder in der Cloud
- Erstellung eines Wiederherstellungsplans
- Verschlüsselung sensibler Daten
- Verwendung von VPNs und verschlüsselten Kommunikationskanälen für externe Zugriffe
- regelmässige Schulungen zu Datenschutz, Phishing-Angriffen und sicheres Verhalten im Arbeitsalltag
- klare interne Richtlinien für den sicheren Umgang mit Personendaten und IT-Systemen
- automatische Updates für Betriebssysteme, Software und Sicherheitslösungen aktivieren
- sofortiges Schliessen von Sicherheitslücken

AUTOR

Dr. iur Lukas Lezzi ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz- und Finanzmarktrecht.

Umgang mit Workation – eine Übersicht

Mobiles Arbeiten im Ausland, auch «Workation» genannt, steht im Zentrum einer sich ständig verändernden Arbeitswelt. Die fortschreitende Digitalisierung ermöglicht, Arbeitstätigkeit neu zu definieren. Die Grenzen für Arbeitnehmer zwischen Büro und Zuhause werden zunehmend undeutlicher. In Zeiten des zunehmenden Fachkräftemangels werden Homeoffice & mobiles Arbeiten im Ausland immer mehr zu einem etablierten Benefit, um Mitarbeiter zu gewinnen. Die rechtlichen, organisatorischen und administrativen Aspekte einer Workation können indes komplex sein, insbesondere wenn Homeoffice-Aktivitäten aus dem Ausland anvisiert sind. Sie erfordern fundierte Kenntnisse der länderspezifischen Regelungen und Vorschriften.

Von Dirk Spacek

Erste Auslegeordnung

Es gibt weder ein gesetzliches Verbot noch ein Recht auf Arbeiten aus dem Ausland. Immerhin besteht eine arbeitsrechtliche Schranke: Ist eine Arbeitstätigkeit aus dem Ausland nicht vereinbarter Bestandteil des Arbeitsvertrags (etwas Reisetätigkeit oder Auslandseinsätze Teil der Arbeitstätigkeit), kann ein Mitarbeiter nicht zu einer «Workation» gezwungen werden. Dies könnte als einseitige Abänderung des Arbeitsvertrags durch den Arbeitgeber angesehen werden. Frequenter ist jedoch das umgekehrte Szenario: Ein Mitarbeiter wünscht sich eine Workation und würde gerne für zwei Monate von seiner Berghütte im Schwarzwald aus arbeiten oder wieso nicht gleich von den Malediven? Mangels gesetzlicher Regelungen treffen Arbeitgeber häufig eigene Regelungen über die Zulässigkeit von Auslandstätigkeiten: Zu regeln sind z. B.: Verpflichtung zu Verschwiegenheit und Datenschutz, Pflicht des Arbeitnehmenden zur Dokumentation der Arbeitszeit, Informationspflichten über den Aufenthalt, welche Arbeitsmittel der Arbeitgeber zur Verfügung stellt, ob eine zeitliche Befristung für die Arbeit im Ausland besteht und inwieweit eine Rückkehrpflicht besteht. Da ein Arbeitnehmer keinen Rechtsanspruch auf eine Auslandsarbeitstätigkeit hat, kann der Arbeitgeber diese auch untersagen. Eine Pflicht des Arbeitgebers zur Rücksichtnahme auf die Interessen des Arbeitnehmers auf eine Workation (wenn dem im Vorfeld nicht zugestimmt wurde) ist nicht leicht argumentativ zu bewerkstelligen. Dies dürfte auch dann gelten, wenn der Lebenspartner des Arbeitnehmers im Ausland lebt und dadurch die familiäre Nähe erschwert sei. Eine Workation bedarf einer individuellen Vereinbarung oder eines kollektiven Konsens im Sinne einer offiziellen Policy gemäss der Mitarbeiter eine Workation in Anspruch nehmen können.

Diverse Rechtsvorschriften beim mobilen Arbeiten aus dem Ausland

Über das Vorgenannte hinaus bestehen diverse Rechtsvorschriften im Aus- und Inland, welche bei der Implementierung einer Workation beachtet werden müssen. Zu erwähnen sind z. B. Fragen der Aufenthalts- und Arbeitserlaubnis, Doppelbesteuerungsabkommen, Aspekte der Sozialversicherung sowie z. B. die Verordnung (EG) Nr. 593/2008 zum anwendbaren Arbeitsrecht.

Die Freizügigkeit in den Ländern der Europäischen Union (EU) und der Europäischen Freihandelszone (EFTA) bietet Arbeitnehmenden mit Wohnsitz in der Schweiz theoretisch die Möglichkeit, ihre Arbeit von verschiedenen europäischen Ländern aus in Telearbeit zu erledigen.

In der Praxis muss sich der Arbeitgeber jedoch ordnungsgemäss über die rechtlichen Bedingungen für die Distanzarbeit eines Arbeitnehmers aus dem Ausland informieren, um potenziell unerwünschte Folgen zu vermeiden. Es sind insbesondere Folgen für die Besteuerung, die Anmeldung bei den Sozialversicherungen und die davon abhängigen Leistungen, den Datenschutz sowie Besonderheiten für entsandte Arbeitnehmende zu berücksichtigen. Empfohlen wird auch, im Arbeitsvertrag festzulegen, welches Arbeitsrecht für die Beziehung zwischen Arbeitgeber und Arbeitnehmer gilt sowie in welchem Mass Homeoffice aus dem Ausland gestattet wird.

Wenn eine in der Schweiz wohnhafte und beschäftigte Person beschliesst, aus einem Mitgliedstaat der EU oder der EFTA in Telearbeit zu arbeiten, bleibt sie in der Schweiz, in ihrem Kanton und ihrer Wohnsitzgemeinde steuerpflichtig, sofern sie nicht mehr als 183 Tage am Stück in dem Gaststaat verbringt. Sie muss zudem weiterhin ihren offiziellen Wohnsitz in der Schweiz haben und den Lohn vom in der Schweiz ansässigen Arbeitgeber erhalten. Wird diese Frist überschritten, hat der Gaststaat das Recht, die Einnahmen des Arbeitnehmers, der sich in seinem Gebiet aufhält, nach seiner eigenen Gesetzgebung zu besteuern. Für kleine Unternehmen, die weitgehend Workation-Aktivitäten ge-

statten, kann der verlängerte Aufenthalt mehrerer Arbeitnehmer in einem anderen Staat (der Grenzwert variiert von Land zu Land) den tatsächlichen Ort der Niederlassung des Unternehmens unter Umständen infrage stellen. Der Gaststaat könnte zu dem Ergebnis kommen, dass das Unternehmen innerhalb seiner Rechtsordnung tätig ist. Dies kann je nachdem steuerliche Auswirkungen haben, etwa die Besteuerung eines Teils der Gewinne im Gastland anstelle des gewöhnlichen Wohnsitzlands.

Genau wie die Staaten der EU und der EFTA nimmt die Schweiz am europäischen System zur Koordinierung der Sozialversicherungen teil, das für Bürgerinnen und Bürger aus der Schweiz und den EU-/EFTA-Staaten gilt. Ein Arbeitnehmer ist grundsätzlich nur einem einzigen Sozialversicherungssystem unterstellt, in der Regel dem System des Staats, in dem er arbeitet. Der Arbeitnehmer, der seinen gewöhnlichen Wohnsitz in der Schweiz hat und dort mindestens 25% seiner Arbeitszeit leistet, bleibt den Schweizer Sozialversicherungen unterstellt (Verordnung (EG) Nr. 883/2004 des Europäischen Parlaments und des Rates vom 29. April 2004 zur Koordinierung der Systeme der sozialen Sicherheit, Art. 13). Sind diese Voraussetzungen nicht mehr erfüllt, muss der Schweizer Arbeitgeber gegebenenfalls Sozialbeiträge an die zuständige Stelle im Ausland abführen. Die Sozialbeiträge können im Ausland höher sein als in der Schweiz. Für den Arbeitgeber empfiehlt sich daher eine umfassende Vorprüfung, falls zahlreiche seiner Arbeitnehmer in substantiellem Ausmass vom Ausland aus für ihn im Rahmen einer Workation tätig werden.

Datenschutz bei Workation im Ausland

Gemäss dem revidierten Schweizer Datenschutzgesetz (DSG) hat der Arbeitgeber über angemessene technische und organisatorische Massnahmen für den Schutz und die Sicherheit der ihm anvertrauten Daten (Unternehmen, Beschäftigte, Kunden usw.) Sorge zu tragen. Wenn ein Arbeitnehmer im Ausland arbeitet, bleibt der Arbeitgeber aber für die Informationssicherheit und den Datenschutz verantwortlich. Folglich muss der Arbeitgeber eine hinreichend zuverlässige Software bereitstellen, die an die Bedürfnisse seines Unternehmens angepasst ist. Bei Telearbeit im Ausland sollte die Bearbeitung personenbezogener Daten, die in der Schweiz gehostet werden, nur über eine gesicherte Verbindung im virtuellen privaten Netzwerk (VPN) erfolgen. Ausserdem wird von jedem Arbeitnehmer erwartet, dass er keine personenbezogenen/vertraulichen Daten an Dritte offenlegt oder verfügbar macht (im Ausland oder nicht im Ausland). Das DSG findet grundsätzlich auch ausserhalb des Schweizer Staatsgebiets Anwendung, wenn die bearbeiteten Daten Unternehmen oder Personen betreffen, deren Sitz bzw. Arbeitsplatz sich in der Schweiz befindet. Die Tatsache, dass ein Arbeitnehmer, dessen Arbeitsplatz sich gewöhnlich in der Schweiz befindet, nun von der EU aus im Homeoffice arbeitet, ist derzeit kein hinreichendes Kriterium für die Anwendbarkeit der Europäischen DSGVO. Die geltende Gesetzgebung sieht bei Fahrlässigkeit keine strafrechtlichen Konsequenzen vor. Absichtliche Verstösse können jedoch

DATENSCHUTZ

WEKA Praxis-Seminar

WEKA

Cloud Services und IT-Projekte vertraglich absichern

Verträge für Ihre IT-Lösungen und Services rechtssicher abschliessen

IT-Leistungen sind heute weitgehend standardisiert in der Form von Standardprodukten oder Services. Umso wichtiger ist es zu wissen, was branchenüblich ist. Bei der Beurteilung und Verhandlung umfangreicher Dokumente kann Sie KI unterstützen.

Nächste Termine

- Mittwoch, 4. Juni 2025
- Dienstag, 11. November 2025

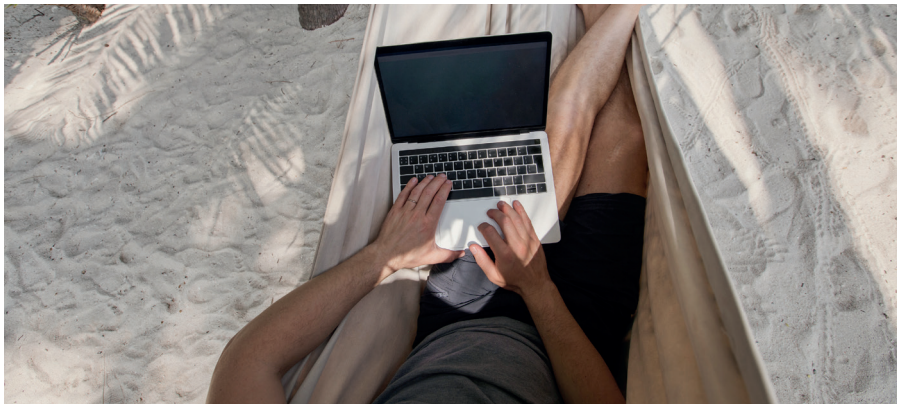
Dauer und Ort: 1 Tag, 09:00–16:30 Uhr
Zürich, Zentrum für Weiterbildung der Uni Zürich

Seminarleitung: Dr. iur. Urs Egli

IT-Verträge Best Practice

An diesem Seminar zeigt Ihnen unser Fachexperte, worauf es bei IT-Verträgen ankommt. Sie erfahren im direkten Praxisvergleich, welche rechtlichen Bedingungen im schweizerischen IT-Markt üblich sind und welche Verhandlungsergebnisse sie realistischerweise erzielen können. Gegenüber dem obersten Leitungsgremium eines Unternehmens oder einer öffentlichen Beschaffungsstelle können Sie kompetent über die rechtlichen Rahmenbedingungen und die mit IT-Leistungen verbundenen Risiken Auskunft geben.

Jetzt informieren und anmelden:
www.praxisseminare.ch oder Telefon 044 434 88 34



mit strafrechtlichen Sanktionen bis zu CHF 250 000.– gegen die verantwortlichen Personen im Unternehmen sanktioniert werden.

Die Europäische DSGVO gilt in allen EU-Ländern und EWR-Ländern (Norwegen, Island und Liechtenstein) und gilt aus Sicht der Schweiz als angemessener Datenschutzstandard. Ein Aufenthalt von Arbeitnehmern im EU-Ausland ist deshalb wenig problematisch. Dasselbe gilt auch für andere Länder mit einem Angemessenheitsbeschluss, weil dort ebenfalls ausweislich ein angemessenes Datenschutzniveau besteht. Schwieriger wird es, wenn Mitarbeiter sich nicht im EU-Ausland befinden (d. h. in unsicheren Drittländern). In solchen Fällen bedarf es grundsätzlich für Datenübermittlungen aus der Schweiz an die im Ausland befindlichen Mitarbeiter zusätzlicher angemessener Schutzmassnahmen. Denn eine Übermittlung an ein unsicheres Drittland liegt bereits vor, wenn Daten aus einem unsicheren Drittland abgerufen werden können. Folgende Schutzmassnahmen sollten diesfalls jedenfalls ins Visier genommen werden:

- IT-Geräte sollten verschlüsselt werden. Das gilt auch für die vom Arbeitgeber herausgegebenen USB-Sticks. Der Zugriff auf das Betriebssystem sollte mit einem Kennwort versehen sein.
- IT-Systeme sollten durch eine Zwei-Faktor-Authentifizierung gesichert sein.
- Mitarbeiter sollten verpflichtet werden, stets den Bildschirm bei Verlassen des Arbeitsgeräts zu sperren und die Geräte immer entweder bei sich oder in einem zugangsgesperrten Raum zu verwahren.
- Daten sollten zentral in der Schweiz gespeichert bleiben und nur bei Bedarf vom Mitarbeiter auf lokale Rechner/Hardware heruntergeladen werden (remote-access ohne separate Datenkopie im Ausland).
- Zugriffe auf die Firmen-IT-Infrastruktur sollten nur über auf ausreichende Belastbarkeit getestete VPNs möglich sein, und die Netzwerkeinstellungen der IT-Geräte sollten einen Zugriff auf das Internet nur über die Firmen-VPN zulassen.
- Und es sollte stets eine Sichtschutzfolie beim mobilen Arbeiten verwendet werden.

Nach Dafürhalten des Autors ist das Unterzeichnen von sogenannten Datentransferverträgen mit den Arbeitnehmern im Ausland (sofern diese in unsicheren Drittländern befindlich wären wie z. B. USA, Indien etc.) entbehrlich bzw. erscheint etwas «gekünstelt» vorgeschoben. Die Arbeitnehmer qualifizieren nach Auffassung des Autors nicht als unabhängige Vertragspartner im Ausland im Sinne von Art. 16 DSG (mit solchen sollten grundsätzlich solche Datentransferverträge abgeschlossen werden). Sie sind interne Mitarbeiter des Unternehmens, d. h. in die Organisation des Schweizer Unternehmens über arbeitsvertragliche Verpflichtungen zur Vertraulichkeit unter schweizerischem Recht eingebunden. Anders wäre dies wohl zu beurteilen, wenn ein Schweizer Unternehmen von vornherein mit reinen Freelancern im Ausland Verträge abschliesst (z. B. auf Auftragsbasis).

Fazit

Workation bietet neue, flexiblere Möglichkeiten der Arbeitsgestaltung für mobile Arbeitnehmer. In Zeiten des zunehmenden Fachkräftemangels werden Homeoffice & mobiles Arbeiten im Ausland immer mehr zu einem möglichen Vorteil, um Mitarbeiter zu gewinnen (z. B. ein Teilzeitmitarbeiter aus dem Nachbarland, der aus familiären Gründen von dort aus ausreichend arbeiten können möchte). Die rechtlichen, organisatorischen und administrativen Aspekte einer Workation sind aber komplex und sollten gut überdacht sein. Nebst arbeitsrechtlichen, steuerrechtlichen und sozialversicherungsrechtlichen Aspekten sollten auch angemessene Vorkehrungen im Bereich Datenschutz und Informationssicherheit getroffen werden. Die wesentlichsten zu beachtenden Punkte sind: (i) Klärung eines Anspruchs (wenn gegeben) und der Konditionen einer Workation für Arbeitnehmer, (ii) Vorprüfung steuerrechtlicher Auswirkungen im Ausland beim Auslandseinsatz mehrerer Arbeitnehmer im Rahmen einer Workation (sowohl für das Unternehmen als auch für den betroffenen Mitarbeiter selbst), (iii) Vorprüfung sozialversicherungsrechtlicher Auswirkungen für den Arbeitnehmer (insbesondere Verhinderung, dass eine Sozialversicherungsabgabe im Ausland erforderlich wird) und (iv) Sicherstellung der Einhaltung des Datenschutzes (insbesondere wenn Mitarbeiter aus unsicheren Drittländern ohne angemessenen Datenschutz mit Zugriff auf Datensysteme tätig werden).

AUTOR

Dirk Spacek, Dr. iur., LL.M., ist Partner in der internationalen Anwaltskanzlei CMS (Schweiz). Er ist Spezialist für Medien-, Technologie (IT) und Immaterialgüterrecht. Er berät Unternehmen vorwiegend in technologieaffinen Rechtsfragen.

Datensicherheit bei Auftragsbearbeitern

Wer IT-Services oder andere Datenverarbeitungsprozesse auslagert, verlässt sich oft darauf, dass die Datensicherheit vom Dienstleister sichergestellt wird. Doch wie sieht das in der datenschutzrechtlichen Praxis aus? Dieser Artikel beleuchtet die wesentlichen Aspekte der Datensicherheit bei Auftragsbearbeitern und gibt Handlungsempfehlungen für Verantwortliche.

Von Simon Schneiter

DAS WICHTIGSTE IN KÜRZE

- **Verantwortung kann nicht outgesourct werden.** Der Verantwortliche muss sich vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.
- **Vertragliche Absicherungen der Datensicherheit sind zu empfehlen.**
- **Vertrauen ist gut, Kontrolle ist besser.** Abhängig vom Risiko empfiehlt es sich, die Umsetzung der Sicherheitsmassnahmen zu überprüfen oder überprüfen zu lassen. Zertifikate und Prüfberichte von Dritten können helfen, müssen aber korrekt interpretiert werden.

Die Auslagerung von IT-Services und Datenverarbeitungsprozessen unterschiedlicher Art ist heutzutage eher die Norm als die Ausnahme. Kaum ein Unternehmen betreibt heutzutage noch seine ganze IT selbstständig. Der Verantwortung für die Datensicherheit entledigt sich das outsourcende Unternehmen damit aber nicht.

Rechtliche Betrachtung

Gemäss Gesetz sind der Verantwortliche und der Auftragsbearbeiter gleichermassen in der Pflicht, für eine adäquate Datensicherheit zu sorgen. Das Schweizer Datenschutzgesetz (DSG) verlangt jedoch explizit, dass der Verantwortliche sich vergewissern muss, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten. Dabei muss die Datensicherheit dem Risiko angemessen sein und durch geeignete technische und organisatorische Massnahmen sichergestellt werden.

In der Praxis bedeutet dies, dass der Verantwortliche verpflichtet ist, den Auftragsbearbeiter sorgfältig auszuwählen, die Datenbearbeitung vertraglich zu definieren und gegebenenfalls auch zu überwachen.

Die Datenschutzverordnung (DSV) spezifiziert, wie Schutzbedarf und Risiko zu beurteilen sind und welche technischen und organisatorischen Massnahmen durch den Verantwortlichen und den Auftragsbearbeiter vorzusehen sind. Wobei die in der Verordnung formulierten Massnahmen eher Sicherheitsziele darstellen, deren konkrete Umsetzung es individuell zu definieren gilt.

Vertragliche Absicherung

Sofern eine Auftragsdatenbearbeitung nicht bereits durch ein Gesetz vorgesehen ist, bedarf es einer vertraglichen Regelung zwischen dem Verantwortlichen und dem Auftragsbearbeiter. Neben der Art und dem Umfang der Datenbearbeitung lässt sich in solchen Verträgen auch die Datensicherheit regeln, indem etwa technische und organisatorische Massnahmen als Vertragsbestandteil festgehalten werden. Während dies rechtlich gesehen sinnvoll ist, kann es in der Praxis gewisse Stolperfallen geben. So müssen bereits zu Beginn, wenn die Massnahmen definiert werden, beide Vertragspartner diese auch verstehen und beurteilen können – dazu ist meist entsprechendes Fachwissen notwendig. Zudem gilt es zu bedenken, dass sich solche Massnahmen über die Zeit auch ändern können, wodurch die entsprechenden vertraglichen Regelungen anzupassen wären, sofern solche Änderungen nicht bereits über

GÄNGIGE ZERTIFIZIERUNGEN UND PRÜFBERICHTE

- **ISO 27001:** Einer der gängigsten Standards, nach welchen sich IT-Dienstleister zertifizieren lassen. Zertifiziert wird dabei ein Informationssicherheitsmanagementsystem, d. h. eine Organisation zur Sicherstellung der Informationssicherheit. Das Zertifikat allein sagt noch nichts darüber aus, welche Kontrollen umgesetzt werden und ob diese effektiv sind. Lassen Sie sich mindestens das Statement of Applicability (SoA) zeigen, um zu verstehen, welche Kontrollen eingesetzt werden. Im Idealfall wird ein aktueller Auditbericht zur Verfügung gestellt.
- **SOC 2:** Das «Service and Organization Controls (SOC) 2»-Framework ist zur Prüfung angemessener Datensicherheit von Dienstleistern vorgesehen. Dabei gilt es zu beachten, dass es zwei Arten von Prüfungen und entsprechenden Berichten gibt. Ein «SOC 2 Type I Report» bewertet, ob die Sicherheitskontrollen eines Unternehmens zu einem bestimmten Zeitpunkt angemessen gestaltet sind, während ein «SOC 2 Type II Report» zusätzlich überprüft, ob diese Kontrollen über einen längeren Zeitraum (typischerweise 3–12 Monate) effektiv funktionieren. Type II bietet dadurch eine stärkere Aussage über die tatsächliche Umsetzung und Wirksamkeit der Kontrollen.
- **CSA STAR:** CSA STAR (Security, Trust & Assurance Registry) ist ein von der Cloud Security Alliance entwickeltes Zertifizierungsprogramm, das die Sicherheitskontrollen von Cloud-Dienstleistern anhand von Cloud-spezifischen Prüfpunkten bewertet. Es werden zwei Level unterschieden. «Level One» ist ein sogenanntes Self-Assessment, d. h., die Überprüfung findet durch die geprüfte Organisation selbst statt. «Level Two» bedingt ein Audit durch einen unabhängigen Dritten.

eine entsprechende Klausel abgedeckt sind.

Überprüfung der Datensicherheit

Abhängig vom Risiko empfiehlt es sich, die Umsetzung der vereinbarten Sicherheitsmassnahmen auch zu überprüfen oder überprüfen zu lassen. Dies sowohl vor einem Vertragsabschluss als auch während der Geschäftsbeziehung. Hierzu können mehrere Methoden zum Einsatz kommen.

Kontrolle vor Ort/Lieferantenaudit: Den besten Einblick in die Umsetzung der Sicherheitsmassnahmen gibt eine individuelle Kontrolle beim Auftragsbearbeiter vor Ort, durchgeführt durch geschultes und erfahrenes Personal. Unternehmen, die selbst nicht über die notwendigen Ressourcen verfügen, können Dritte mit einem solchen Audit beauftragen. Es empfiehlt sich, solche Audit-Rechte und die Aufteilung der Kostenfolgen bereits im Vorfeld vertraglich festzuhalten.

Zertifizierungen & Berichte: Viele Dienstleister lassen sich nach gängigen Standards prüfen und/oder zertifizieren. Sie stellen die entsprechenden Zertifikate und Berichte ihren Kunden zur Verfügung, um diesen einen Nachweis über die Wirksamkeit der Sicherheitsmassnahmen zu liefern. Insbesondere die grossen IT-Dienstleister schliessen individuelle Audits und Überprüfungen meist vertraglich aus und verweisen stattdessen auf ihre Zertifikate und Prüfberichte. Für Verantwortliche ist diese Art der Überprüfung ressourcenschonender, als selbstständig Audits durchzuführen oder zu beauftragen. Die Aussagekraft der entsprechenden Nachweise unterscheidet sich jedoch stark (siehe Box). Vorsicht geboten ist besonders dann, wenn ein Anbieter mit Zertifikaten und unabhängigen Audits wirbt, aber (potenziellen) Kunden keinerlei Details dazu bekannt gibt.

Wird Einsicht in Zusatzdokumentation und Prüfberichte gewährt, so ist auf folgende Punkte zu achten:

- Auf welchen Geltungsbereich bezieht sich das Dokument? Sind die aus Sicht Kunde relevanten Services abgedeckt?
- Sind die Dokumente aktuell? Eine Zertifizierung muss meist jährlich erneuert werden, und ein mehrere Jahre alter Prüfbericht hat oft eine geringe Aussagekraft.
- Zu welchen Resultaten kamen die externen Prüfer? Nur weil ein Zertifikat und/oder ein Bericht vorhanden sind, heisst das nicht, dass keinerlei Auffälligkeiten oder Kontrolllücken festgestellt wurden.

Penetrationstests & Schwachstellenanalysen: In einigen Fällen sind Lieferanten auch bereit, Berichte zu technischen Schwachstellenanalysen oder Penetrationstests (Hacking durch selbst beauftragte Spezialisten) mit wichtigen Kunden zu teilen. Mehrheitlich werden solche Dokumente jedoch nicht an Kunden abgegeben. Etwas anders kann es aussehen, wenn dem Dienstleister vorgeschlagen wird, eine solche Analyse als Kunde selbst zu beauftragen und die Kosten zu übernehmen. Die regelmässige Überprüfung der externen Angriffsfläche, sprich der über das Internet zugänglichen Webservices, kann ausserdem über spezialisierte Cloud-Services abonniert werden. Entsprechende Tools scannen bestimmte Webserver oder detektieren alle mit einer bestimmten Domain verbundenen Systeme, um diese anschliessend auf Software- und Konfigurationsschwachstellen zu prüfen und eine passende Bewertung zu präsentieren.

Individuelle Berichterstattung: Zu guter Letzt sei erwähnt, dass sich mit gewissen Dienstleistern auch individuelle Abmachungen treffen lassen, die eine regelmässige Berichterstattung vorsehen, welche auf den Bedarf des Kunden zugeschnitten sind.

Aufwand und Ertrag

Alle diese Methoden zur Prüfung der Datensicherheit sind mit Aufwänden verbunden. Und so stellt sich für den Verantwortlichen die Frage, wie viel Aufwand denn notwendig ist, um den gesetzlichen Anforderungen zu entsprechen. Im Gesetz lässt sich dazu verständlicherweise keine konkrete Antwort finden. Die Datenschutzverordnung verlangt aber, dass bei der Festlegung der technischen und organisatorischen Massnahmen, nebst Schutzbedarf, Risiko und dem Stand der Technik, auch die Implementierungskosten mitberücksichtigt werden. Dies darf allerdings nicht dazu führen, dass aufgrund zu hoher Kosten keine angemessene Datensicherheit gewährleistet wird. Schlussendlich bleibt es Sache des Verantwortlichen, einzuschätzen, wie viel Aufwand notwendig ist, um eine angemessene Datensicherheit beim Lieferanten sicherstellen zu können.

Fazit

Die Datensicherheit muss auch bei einer Auslagerung von Datenbearbeitungstätigkeiten und IT-Services sichergestellt werden. Dieser Verantwortung kann nachgekommen werden, indem einerseits vertragliche Regelungen getroffen werden und andererseits der Auftragsbearbeiter sowohl vor als auch während der Geschäftsbeziehung in angemessener Weise überprüft wird.

AUTOR

Simon Schneiter, M.A. HSG (Informations-, Medien- und Technologiemanagement), Head GRC & Information Security Consulting bei ensec AG.

Dos und Don'ts bei einem Data Breach

Gemäss den neuesten Zahlen des Eidgenössischen Datenschutzbeauftragten (EDÖB) sind von Januar bis November 2024 rund 293 Data-Breach-Meldungen eingegangen, was knapp einer Meldung alle 1,5 Tage entspricht. Vergleicht man die Anzahl der Meldungen an den EDÖB mit den Cybersicherheitsvorfällen, die 2024 an das Bundesamt für Cybersicherheit (BACS) gemeldet wurden – nämlich alle 8,5 Minuten eine Meldung –, scheint die Zahl der an den EDÖB gemeldeten Vorfälle nicht besonders gross. Selbstredend ist nicht jeder Cybervorfall automatisch auch ein Data Breach, und nicht jeder Data Breach löst eine Meldepflicht an den EDÖB aus. Die Zahlen lassen aber vermuten, dass es im Jahr 2024 weitaus mehr relevante Data Breaches gegeben hat, die nicht an den EDÖB gemeldet wurden. Nachfolgend wird erläutert, was ein Data Breach ist und wann ein solcher Vorfall Pflichten nach dem Datenschutzgesetz (DSG) auslöst. Ergänzt werden die Ausführungen mit Handlungsempfehlungen (Dos und Don'ts).

Von Elenor Gyr

Was ist ein Data Breach?

Ein Data Breach ist gemäss der Definition im DSG eine Datensicherheitsverletzung, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Eine Datensicherheitsverletzung kann durch einen technischen oder menschlichen Fehler, aber auch durch Cyberangriffe verursacht werden.

Pflichten bei einem Data Breach nach dem DSG

Ein Data Breach kann regulatorische Pflichten nach sich ziehen. So sieht das DSG zwei verschiedene Pflichten vor: einerseits die Meldepflicht an den EDÖB und andererseits die Pflicht, die betroffene Person zu informieren.

Meldepflicht

Nicht jeder Data Breach muss dem EDÖB gemeldet werden. Notwendig ist ein **voraussichtlich hohes Risiko für die Verletzung der Persönlichkeits- oder Grundrechte der betroffenen Person** (Art. 24 DSG). Die Frage, ob ein voraussichtlich hohes Risiko besteht, ist in der Praxis nicht einfach zu beantworten. Nach dem neusten Leitfaden des EDÖB[1] muss auch dann Meldung erstattet werden, wenn die Risikoanalyse ein entsprechend hohes Risiko nicht ausschliessen kann. In der Beurteilung, ob eine Meldung zu erstatten ist, sind Sofortmassnahmen, welche der/die Verantwortliche zur Schadensbehebung oder -minimierung getroffen hat, nicht zu berücksichtigen. Folgende Kriterien können zur Bestimmung eines hohen Risikos beigezogen werden: Schwere der Folgen und Wahrscheinlichkeit der befürchteten Folgen. Bei der Schwere der Folgen gilt die Faustregel, dass sich das Risiko mit der Sensibilität der Daten erhöht. Die Wahrscheinlichkeitsbeurteilung bemisst sich hingegen bei den am stärksten betroffenen Personen in Relation zum befürchteten Beeinträchtigungspotenzial.

Die Meldung an den EDÖB hat «so rasch als möglich» zu erfolgen.

An die Meldepflicht gekoppelt ist eine **Dokumentationspflicht.** Der/Die Verantwortliche hat den Vorfall umfassend zu dokumentieren und ab Meldezeitpunkt für mindestens zwei Jahre aufzubewahren.

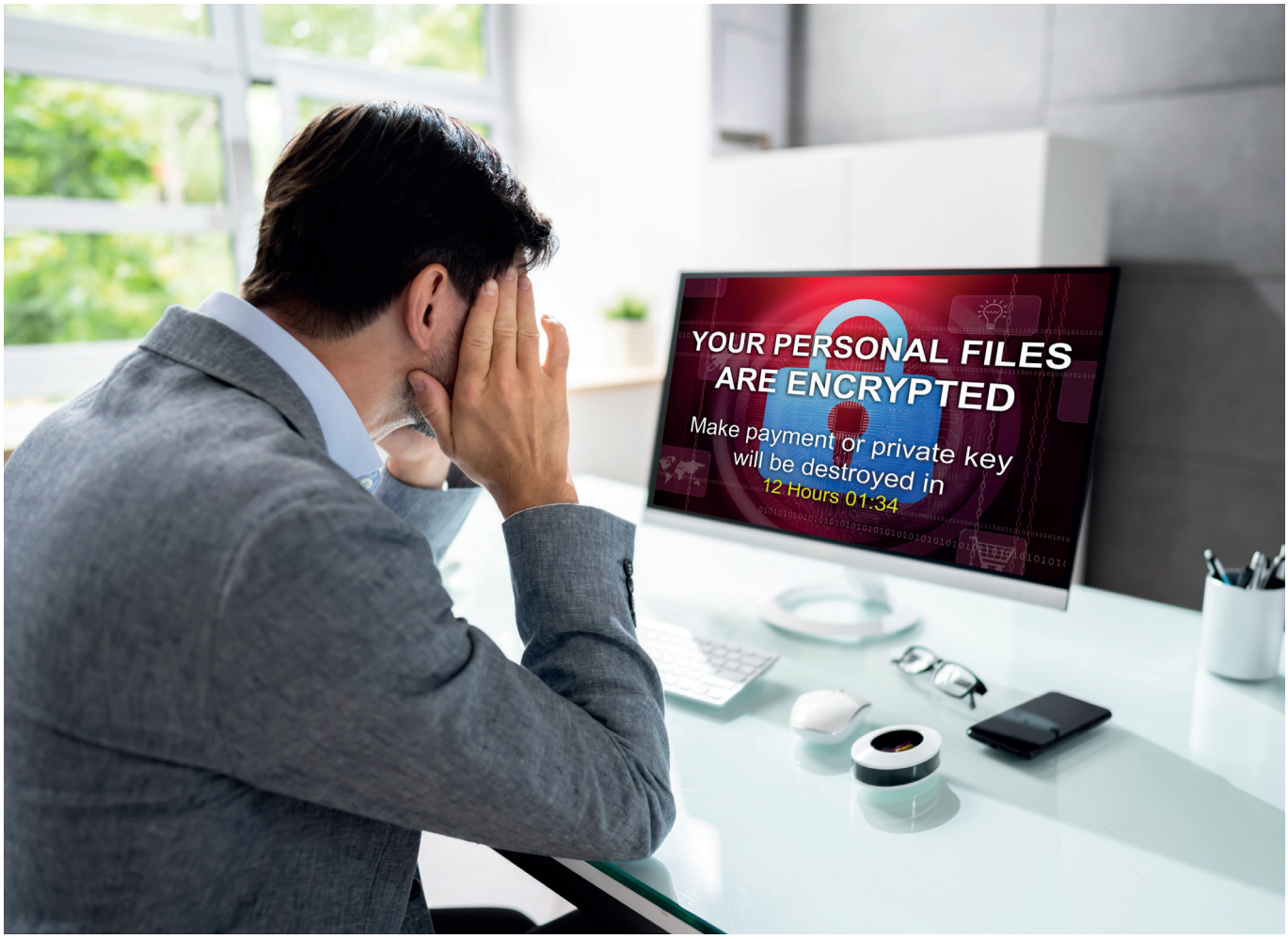
WICHTIGER HINWEIS

- Ein Data Breach ist eine Datensicherheitsverletzung. Dabei werden Personendaten verloren, gelöscht, vernichtet oder verändert oder Unbefugten offengelegt oder zugänglich gemacht.
- Bei einem hohen Risiko für die betroffene Person besteht eine Meldepflicht an den EDÖB.
- Bei einem Schutzbedarf der betroffenen Person besteht eine Informationspflicht an die betroffene Person.

Informationspflicht

Nebst der Meldepflicht an den EDÖB besteht bei einem Data Breach auch eine Pflicht zur Information der betroffenen Person. Voraussetzung dafür ist, dass **die Information zum Schutz der betroffenen Person erforderlich** ist oder der EDÖB dies verlangt. Für die Informationspflicht ist nicht primär ausschlaggebend, ob ein hohes Risiko für die betroffene Person besteht, sondern vielmehr, ob die Person die Information benötigt, um selbst Schutzvorkehrungen zu treffen. Dies ist beispielsweise beim Verlust von Passwörtern, Kreditkartendaten etc. der Fall, bei dem die betroffene Person Passwörter ändern

1 Leitfaden des EDÖB betreffend die Meldung von Datensicherheitsverletzungen und Informationen der Betroffenen nach Art. 24 DSG vom 6. Februar 2025.



oder Kreditkarten sperren muss. Überdies ist gesetzlich vorgegeben, wie die Information an die betroffene Person zu erfolgen hat. Sie muss einerseits in einfacher und verständlicher Sprache verfasst sein. Andererseits müssen folgende Inhalte übermittelt werden: die Art und Folgen der Verletzung; soweit möglich Zeitpunkt, Dauer, Kategorien und ungefähre Anzahl der betroffenen Personendaten; soweit möglich Kategorien und ungefähre Anzahl der betroffenen Personen; getroffene und geplante Massnahmen zur Mangelbehebung und Risikominderung sowie Kontaktangaben einer Ansprechperson.

Weitere Meldepflichten

Nicht nur das DSG, sondern auch andere Gesetze sehen Meldepflichten bei einem Data Breach vor. Schweizer Unternehmen, die unter die Europäische Datenschutz-Grundverordnung (DSGVO) fallen, haben zusätzlich die entsprechenden Meldepflichten zu beachten. Die DSGVO gibt eine Frist von 72 Stunden für Meldungen vor. Es sind zusätzlich die Meldeverfahren und -fristen in den einzelnen Jurisdiktionen zu beachten.

In der Schweiz gibt es zudem für die von der FINMA beaufsichtigten Unternehmen eine Meldepflicht für Cyberattacken, wenn diese eine gewisse Wesentlichkeit aufweisen. Bei einem Data Breach im Sinne des DSG kann dies der Fall sein, wenn durch den Vorfall der (Individual-)Schutz der Kundinnen und Kunden verletzt wird.[2]

Ab dem 1. April 2025 besteht zudem eine Meldepflicht für kritische Infrastrukturen (wie beispielsweise Energieversorger, Netzbetreiber oder Finanzdienstleister) an das Bundesamt für Cybersicherheit (BACS).

To-do: Prävention

Jedes Unternehmen kann von einem Data Breach betroffen sein. Aus diesem Grund ist es zentral, entsprechende Vorkehrungen zu treffen.

Es gilt nicht nur, sich einen umfassenden Überblick über die eigenen Daten (Stichwort: Bearbeitungsverzeichnis), sondern auch über die vertraglich angeschlossenen Dienstleister zu verschaffen. Es müssen Prozesse etabliert werden, die im Krisenfall greifen und unverzügliche Massnahmen auslösen (Reaktionsplan). Interne Abläufe und Verantwortlichkeiten müssen klar geregelt sein. Es ist auch empfehlenswert, externe Dienstleister, wie z. B. Cybersicherheitsexperten oder Anwälte, im Vorfeld zu bestimmen und zu mandatieren, um im Krisenfall keine unnötige Zeit zu verlieren.

2 Art. 29 Abs. 2 FINMAG, FINMA-Aufsichtsmitteilung 05/2020 und 03/2024.

To-do: Umgehende Reaktion

Sobald ein Data Breach bemerkt wird, muss rasch gehandelt werden. Die im Idealfall vorgängig geschaffenen Prozesse können aktiviert werden. Falls keine entsprechenden Prozesse bestehen, empfiehlt es sich, so rasch wie möglich externe Hilfe beizuziehen. Es gilt einerseits die Datensicherheitsverletzung zu beheben und die betroffenen Systeme zu sichern. Gleichzeitig gilt es andererseits zu prüfen, ob regulatorische Meldepflichten bestehen und wie gegenüber Behörden, betroffenen Personen und intern kommuniziert wird.

To-do: Dokumentation

Sofern eine Meldepflicht besteht, muss der Vorfall umfassend dokumentiert werden. Eine Dokumentation des Vorfalls ist jedoch auch empfehlenswert, wenn keine Meldepflicht besteht. Dies ist hilfreich für das interne Reporting, dient aber auch der Etablierung von neuen Prozessen und zu treffenden Massnahmen zur Stärkung der Datensicherheit.

Do:

- Prävention: Prozesse etablieren und Dienstleister auswählen (Reaktionsplan).
- Bei Vorfall: umgehend reagieren, Reaktionsplan aktivieren.
- Nachbearbeitung: Prozesse und Sicherheitsvorkehrungen anpassen.

Don'ts: Ignorieren und Verschweigen

Einen Data Breach zu ignorieren oder zu verschweigen, ist in mehrfacher Hinsicht nicht zu empfehlen. Durch das Ignorieren eines solchen Vorfalls können die Folgen nicht abgeschätzt werden. Dies birgt ein unternehmerisches Risiko, welches zu vermeiden ist.

Der Vorfall sollte zudem zumindest den internen Leitungsorganen offengelegt und die zu treffenden Massnahmen diskutiert werden. Das Ignorieren und Verschweigen eines Vorfalls kann nicht nur rechtliche Konsequenzen nach sich ziehen, sondern zu einem (erheblichen) Reputations- und Vertrauensverlust führen.

Fazit

Fachpersonen sagen oft und gerne: Die Frage ist nicht, ob, sondern wann ein Unternehmen von einem Data Breach betroffen sein wird. Data Breaches sind allgegenwärtig, und es kann jedes Unternehmen treffen. Prävention ist daher das A und O.

AUTORIN

Eleonor Gyr, Dr. iur., Rechtsanwältin, CIPP/-E, ist spezialisiert auf IT-, Gesellschafts- und Finanzmarktrecht und Partnerin der Wirtschaftskanzlei Gyr | Gössi | Olano | Staehelin in Basel.

DATENSCHUTZ

WEKA Praxis-Seminar

WEKA

Künstliche Intelligenz (KI) und Cybersicherheit

Sicherheit und Zuverlässigkeit von KI-Modellen gewährleisten

Im Zeitalter digitaler Transformation wird die KI immer mehr zu einem integralen Bestandteil unserer täglichen Abläufe. Als Verantwortliche/-r für künstliche Intelligenz spielen Sie eine entscheidende Rolle bei der Gewährleistung der Sicherheit dieser technologischen Lösungen. Sie sind verantwortlich für die Analyse und Behandlung von Sicherheitsrisiken, die mit der Implementierung und Nutzung von KI verbunden sind.

Nächste Termine

- Dienstag, 20. Mai 2025
- Donnerstag, 30. Oktober 2025

Dauer und Ort: 1 Tag, 09:00–16:30 Uhr
Zürich, Schweizerisches Institut für Betriebsökonomie

Seminarleitung:
Hermann Escher

Jetzt informieren und anmelden:
www.praxisseminare.ch oder Telefon 044 434 88 34

IMPRESSUM

Verlag: WEKA Business Media AG, Hermetschloostrasse 77, CH-8048 Zürich, www.weka.ch
Herausgeber: Stephan Bernhard
Redaktion: Marco S. Meier
Korrektorat: Margit Bachfischer M.A., Bobingen
Layout/Satz: Tonio Schelker
Publikation: 10 × jährlich, Abonnement: CHF 98.– pro Jahr, Preise exkl. MWST und Versandkosten. Als digitale Publikation erhältlich unter: www.weka-library.ch
Bildrechte: www.istockphoto.com
Bestell-Nr.: 9231

Scannen und bestellen:
Dieser Newsletter ist in gedruckter Form und digital in unserem Online-Shop erhältlich.

Ihre Vorteile
- Fundiertes Praxiswissen der Datenschutzanforderungen
- Lösungen für Datenschutzthemen

www.weka.ch/shop

© WEKA Business Media AG, Zürich, 2025

Urheber- und Verlagsrechte: Alle Rechte vorbehalten, Nachdruck sowie Wiedergaben, auch auszugsweise, sind nicht gestattet. Die Definitionen, Empfehlungen und rechtlichen Informationen sind von den Autoren und vom Verlag auf ihre Korrektheit in jeder Beziehung sorgfältig recherchiert und geprüft geworden. Trotz aller Sorgfalt kann eine Garantie für die Richtigkeit der Informationen nicht übernommen werden. Eine Haftung der Autoren bzw. des Verlags ist daher ausgeschlossen. Wenn möglich verwenden wir immer geschlechtsneutrale Bezeichnungen. Aus Platzgründen oder aufgrund einer besseren Lesbarkeit verwenden wir bei Texten nur eine Schreibweise.