AUS DER PRAXIS | FÜR DIE PRAXIS

Revision des Schweizer Datenschutzgesetzes – Auswirkungen auf Unternehmen

Markus Hugentobler
Dr. iur.
Centre Patronal Bern

Inhalt

DSG

- Neuerungen
  - Begriffe
  - Rollen
  - Aufgaben
- Gemeinsamkeiten und Unterschied betr. DSGVO

Dateninventar

Vorbemerkung zum schweizerischen DSG

Das revidierte schweizerische Datenschutzgesetz (DSG) wird am 1. September 2023 in Kraft treten. Das Gesetz liegt bereits seit längerem vor, doch mussten die Verordnungstexte noch ausgearbeitet werden.

Das DSG übernimmt inhaltlich ca. 80% der Regelungen der DSGVO, ist aber vom Umfang her viel schlanker abgefasst.

Vorbemerkung zum schweizerischen DSG

Das DSG schützt nur noch Personendaten von natürlichen Personen (Art. 2 Abs. 1 nDSG).

Vereine und Stiftungen fallen also nicht mehr unter den Anwendungsbereich, müssen jedoch umgekehrt – unter Strafandrohung nach Art. 60 ff. nDSG – als Datenbearbeiterinnen eine Reihe von Pflichten (Art. 19 ff. nDSG) erfüllen.

Umsetzung revidiertes DSG

Beispiel

Ihre Arbeitswoche haben Sie als HR-verantwortliche Person problembeladen begonnen.

Am Montagmorgen kam Mitarbeiter Anton Schussel zu Ihnen ins Büro und beichtete mit gesenktem Kopf, er hätte sein – entgegen klarer Arbeitgeberweisung – nicht passwortgeschütztes Geschäfts-Smartphone im Zug liegen lassen.

Umsetzung revidiertes DSG

Beispiel

Gleich nach der Znüni-Pause vernahmen Sie von Ihrer Personalassistentin Therese Schnell, sie hätte aus Versehen ein Rekrutierungsdossier mit Auswertungsberichten per E-Mail an einen falschen Empfänger ausserhalb des Unternehmens geschickt.

Am gleichen Nachmittag finden Sie heraus, dass Ihr geschäftliches E-Mail-Konto gehackt wurde.

Der ganzen EDV-Probleme überdrüssig denken Sie: “Dumm gelaufen!” und gehen zur Tagesordnung über.

Umsetzung revidiertes DSG

Fragestellung zum Beispiel

Haben Sie richtig gehandelt oder wären besondere Massnahmen zu treffen?

Welche Massnahmen?

AUS DER PRAXIS | FÜR DIE PRAXIS

Revidiertes Datenschutzgesetz DSG

Neue Begriffe

Begriffe
(Art. 5 DSG)

- **Betroffene Person:** Natürliche Person, über die Daten bearbeitet werden. D.h. geschützte Person.
- **Bearbeitung:** Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten z.B. Erfassen, Ordnen, Speichern, Übermitteln, Löschen.

Wichtig

- Juristische Personen (auch Vereine und Stiftungen) sind weder vom DSG noch von der DSGVO geschützt; im Gegenteil stehen sie in der Datenschutzpflicht.
- Jeder Umgang mit Personendaten ist erfasst, auch wenn Daten beispielsweise „nur“ gespeichert werden.

Datenschutz durch Technik und Voreinstellungen

- **Privacy by Default** wird durch **datenschutzfreundliche Voreinstellungen** Genüge getan.

  Das bedeutet insbesondere, dass Systeme so aufgebaut werden, dass nur jene Daten erhoben werden können, welche für die Erfüllung des Verarbeitungszwecks notwendig sind.

→ Der Bearbeiter verfügt noch nicht über die betreffenden Daten.

Datenschutz durch Technik und Voreinstellungen

- **Privacy by Design** bedeutet, dass die Grundsätze des DSG **durch geeignete Technik** sichergestellt werden. Dazu gehören zum Beispiel:
  - rasche Pseudonymisierung oder Anonymisierung, wenn Personenbezug nicht notwendig;
  - regelmässige Löschung von Daten, wenn möglich;
  - der Betroffene gibt die zu bearbeitenden Daten selber frei (Einwilligung durch Anklicken der freizugebenden Daten).

  → Der Datenbearbeitungsprozess ist bereits im Gange.

Profiling
(Art. 5 DSG)

- Der Begriff des **Persönlichkeitsprofils** wurde aus dem DSG gelöscht. Neu wird der Begriff des Profilings verwendet.
- **Profiling** bedeutet eine automatisierte Auswertung von Personendaten, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, zu analysieren oder vorherzusagen.
- Beim Profiling handelt es sich um einen Datenbearbeitungsprozess, somit um einen dynamischen Vorgang. Die Digitalisierung vieler Prozesse basiert auf der Bildung von Profilen.
- Ist eine **Einwilligung** erforderlich, so muss diese **ausdrücklich** gegeben werden.

Automatisierte Einzelentscheidung
(Art. 21 DSG)

- Wird eine Entscheidung **ausschliesslich** mit automatisierten Methoden getroffen, liegt eine automatisierte Entscheidung im Einzelfall vor.
- Ist sie mit **Rechtsfolgen** für die betroffene Person verbunden oder wird sie erheblich davon beeinträchtigt, so muss
  - die betroffene Person **informiert** werden und auf Antrag die Möglichkeit erhalten, **ihren Standpunkt darzulegen;**
  - die Entscheidung auf Verlangen der betroffenen Person **von einer natürlichen Person geprüft werden.**
- Ausnahmen bestehen bei einem unmittelbaren Zusammenhang mit dem Abschluss oder Abwicklung eines Vertrags oder bei Einwilligung der betroffenen Person.

Beispiele

- Wird ein automatisiertes **Personalrekrutierungstool** eingesetzt, welches die Bewerbungsunterlagen in positiv und negativ unterteilt, liegt eine automatisierte Einzelentscheidung vor, wenn die negativ bewerteten Kandidatinnen und Kandidaten gestützt darauf ohne weiteres eine Absage erhalten.
- Offene Fragen:
  - Ausnahmefall und somit weder Information noch Überprüfung durch eine natürliche Person? Gemäss der Lehre gilt Art. 328b OR als zwingende Norm bereits anlässlich der Rekrutierung.
  - Kein Rechtsanspruch auf Anstellung: Rechtsfolgen für die bzw. Erheblichkeit der Beeinträchtigung der betroffenen Person?

Beispiele

- Analysiert eine **Bank** die Daten ihrer Kunden mittels automatisierter Verfahren, um die Kunden je nach ihrem Einkommen und Vermögen in verschiedene Kategorien A, B und C einzuteilen, handelt es sich um ein Profiling.
- Doch nur wenn die Entscheidung beispielsweise über einen Kreditantrag automatisiert und ohne Eingreifen des Kundenberaters bzw. der Kundenberaterin (oder eines anderen Mitarbeitenden der Bank) erfolgt, dann handelt es sich um eine automatisierte Einzelentscheidung.

Empfehlung: Prüfen Sie bei der Digitalisierung von Prozessen, ob Sie automatisierte Entscheidungen im Einzelfall treffen.

AUS DER PRAXIS | FÜR DIE PRAXIS

Revidiertes Datenschutzgesetz DSG

Neue Rollen

Rollenverteilung
(Art. 5 DSG)

- **Verantwortlicher**: Natürliche oder juristische Personen („private Person“) oder Behörden, die über die Zwecke und die Mittel der Verarbeitung von personenbezogenen Daten entscheiden.
- **Auftragsbearbeiter**: Natürliche oder juristische Personen („private Person“) oder Behörden, die im Auftrag des Verantwortlichen solche Daten verarbeiten (Dienstleister, Provider).

Datenschutzberaterin oder -berater
(Art. 10 DSG)

- Freiwillig
- Ernennung durch Verantwortlichen (dieser bleibt verantwortlich)
- Anforderungen
  - Mitarbeitender oder externe Person
  - Fachkompetenz (Datenschutzrecht allg., Informationssicherheit, Datenbearbeitung)
  - Ausschluss von Interessenskonflikten
- Stellung
  - Fachliche Unabhängigkeit
  - Keine Weisungsgebundenheit

Datenschutzberaterin oder -berater
(Art. 10 DSG)

- Bezeichnung als „Datenschutzberaterin oder –berater“
- Meldung der Kontaktdaten an den EDÖB
- Veröffentlichung der Kontaktdaten (Single Point of Contact)
  - Website (E-Mail-Adresse z.B.: datenschutz@xy.ch)
  - Datenschutzerklärung
- Befreiung von der Pflicht zur Vorlage der Datenschutz-Folgenabschätzung beim EDÖB (Art. 23 Abs. 4 DSG)

Die administrativen Erleichterungen für Unternehmen mit einem Datenschutzberater sind also nur gering.

AUS DER PRAXIS | FÜR DIE PRAXIS

Revidiertes Datenschutzgesetz DSG

Neue Aufgaben

Verzeichnis der Bearbeitungstätigkeiten (Dateninventar)

(Art. 12 DSG)

„Der Verantwortliche und Auftragsbearbeiter führen je ein Verzeichnis ihrer Bearbeitungstätigkeiten.“

- Ersetzt die Pflicht zur Meldung der Datensammlungen an den EDÖB.
- Das Dateninventar ist somit ein **internes Dokument.**
- **Schriftliche Darstellung** der **wesentlichen Informationen** zu allen Datenbearbeitungen des Verantwortlichen oder des Auftragsbearbeiters: Wer bearbeitet welche Daten zu welchem Zweck?
- Es wird **nicht** verlangt, **einzelne Bearbeitungsschritte** zu beschreiben.
- Dennoch ist die Erstellung eines Dateninventars sehr **aufwändig**.

Auswirkungen des Dateninventars auf die Praxis

- Weil **alle Datenbearbeitungen** dokumentiert und zusätzliche Informationen erfasst werden müssen, wird der Dokumentationsaufwand grösser.
- Weil dem EDÖB auf Anfrage Datenübermittlungen in Drittstaaten gemeldet werden müssen, die auf **Ausnahmen** nach Art. 17 Abs. 1 Bst. b Ziff. 2, c und d beruhen (z.B. Abschluss und Abwicklung eines Vertrages, Gerichtsverfahren [Art. 17 Abs. 2 DSG]), müssen diese zusätzlich dokumentiert werden.

Auswirkungen des Dateninventars auf die Praxis

- Der Bundesrat sieht für Unternehmen mit **weniger als 250 Mitarbeitenden** Ausnahmen vor, sofern ihre Datenbearbeitungen kein hohes Risiko aufweisen (Art. 12 Abs. 5 DSG). Doch letzteres wird oft der Fall sein.
- Nur die Verweigerung der Herausgabe des Verzeichnisses an den EDÖB ist strafbar (Art. 60 Abs. 2 DSG), nicht jedoch das fahrlässige Unterlassen oder die fehlerhafte Erstellung.

Datenschutz-Folgenabschätzung
(Art. 22 DSG)

„Der Verantwortliche erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. […].“

- Die Datenschutz-Folgenabschätzung (DSFA) dient der systematischen Risikoeindämmung. Risiken müssen erkannt und anhand angemessener Mittel verringert werden.
- Die Pflicht besteht für den Verantwortlichen; der **Auftragsbearbeiter** muss **keine** DSFA durchführen. Er sollte vertraglich verpflichtet werden, den Verantwortlichen zu unterstützen.

Datenschutz-Folgenabschätzung
(Art. 22 DSG)

- Um ihren Zweck zu erfüllen, muss die DSFA **vor der ersten Datenbearbeitung** erfolgen. Ähnliche Verarbeitungsvorgänge mit einem ähnlichen Risiko können gemeinsam beurteilt werden.
- Die Verletzung der Pflicht zur Durchführung einer DSFA ist **nicht strafbar.**
- Der EDÖB kann den Verantwortlichen zur **Durchführung einer DSFA** (Art. 51 Abs. 3 lit. d DSG) oder zur **Herausgabe der DSFA** (Art. 50 Abs. 1 lit. a DSG) verpflichten.

Datenschutz-Folgenabschätzung: Ausnahmen
(Art. 22 Abs. 4 und 5 DSG)

- Verantwortliche, die Personendaten **ausschliesslich** in Erfüllung einer gesetzlichen Pflicht bearbeiten, müssen dafür keine DSFA durchführen (z.B. Banken oder Spielcasinos, die Daten zur Bekämpfung von Geldwäscherei bearbeiten müssen).
- Private Verantwortliche können von der Durchführung einer DSFA absehen, wenn sie nach Art. 13 DSG zertifiziert sind, oder wenn sie sich an einen Verhaltenskodex nach Art. 11 DSG halten. **ABER:**

Datenschutz-Folgenabschätzung: Ausnahmen
(Art. 22 Abs. 4 und 5 DSG)

- Die Ausnahme der **Zertifizierung** ist in der Praxis ohne Relevanz, da eine Datenschutzzertifizierung (z.B. nach VDSZ) die Durchführung einer DSFA zwingend vorsieht (sog. Konformitätsmanagement).
- Ein **Verhaltenskodex** befreit nur dann von der Durchführung einer DSFA, wenn dieser selbst auf einer DSFA beruht, Schutzmassnahmen für die betroffenen Personen vorsieht und dem EDÖB vorgelegt wurde.

→ Die Katze beisst sich sozusagen wiederholt in den Schwanz.

Konsultation des EDÖB
(Art. 23 DSG)

- Sollte **trotz der ergriffenen Massnahmen** ein hohes Risiko für die betroffenen Personen bleiben, muss der EDÖB konsultiert werden.
- Der EDÖB nimmt innerhalb von 2 Monaten Stellung (Verlängerung auf 3 Monate möglich).
- Der EDÖB kann **Massnahmen** vorschlagen, wenn er Einwände gegen die geplante Datenbearbeitung hat. Dafür kann er dem Verantwortlichen **Gebühren** in Rechnung stellen (Art. 59 Abs. 1 lit. c DSG).
- Der EDÖB muss nicht konsultiert werden, wenn die DSFA der Datenschutzberaterin oder dem -berater vorgelegt wurde.

Auswirkungen auf die Praxis

- In der Praxis wird die **Definition des hohen Risikos** ausschlaggebend dafür sein, wieviel Aufwand die Unternehmen in Zukunft mit DSFA haben werden.
- Das DSG geht über die DSGVO hinaus, da beispielsweise bei einem Profiling immer eine DSFA durchzuführen ist, obwohl nicht jedes Profiling automatisch mit einem hohen Risiko für die betroffenen Personen verbunden ist. Insofern ist die Formulierung von Art. 23 DSG irreführend.
- Entgegen der DSGVO ist im DSG nicht vorgesehen, gewisse Datenbearbeitungen generell von der Pflicht zur Durchführung einer DSFA auszunehmen.

Auswirkungen auf die Praxis

- Nicht nur die eigentliche Durchführung der DSFA sondern bereits die Klärung, ob eine solche durchgeführt werden muss und das Ergebnis dieser Prüfung, sollten **dokumentiert** werden (Schwellwertanalyse).
- An die **Form der Dokumentation** werden keine besonderen Anforderungen gestellt, weshalb sowohl die physische als auch die elektronische Form zulässig sind.

Meldung von Datensicherheitsverletzungen
(Art. 24 DSG)

- **Datensicherheitsverletzung**: Verletzung der Sicherheit, die dazu führt, dass Personendaten verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden (Art. 5 lit. h DSG).
- Verstösse gegen Massnahmen zur Datensicherheit müssen durch Verantwortliche dokumentiert und dem EDÖB **gemeldet** werden.

Meldung von Datensicherheitsverletzungen
(Art. 24 DSG)

- Wenn es der EDÖB es verlangt bzw. wenn voraussichtlich ein hohes Risiko für die betroffenen Personen besteht, muss auch die betroffene Person informiert werden.
- **Auftragsbearbeiter** müssen alle Datensicherheitsverletzungen dem Verantwortlichen ohne Verzug melden.
- **Empfehlung**: Es muss ein Prozess eingeführt werden, um die Datensicherheitsverletzungen zu dokumentieren, zu bewerten und in den vorgesehenen Fällen zu melden.

Meldepflicht bei Datensicherheitsverletzungen

Prüfschema

Unbefugte Datenverarbeitung?

- Nein: Keine Meldepflicht
- Ja: Datenverlust?
    - Ja: Meldepflicht
    - Nein: Risiko für Betroffene?
        - Nein: Keine Meldepflicht
        - Ja: Meldepflicht

Meldepflicht bei Datensicherheitsverletzungen

Grundlagen

- EU: Benachrichtigung der Aufsichtsbehörde unverzüglich und möglichst **binnen 72 Stunden**.

  CH: möglichst rasch an den EDÖB, Art. 24 Abs. 1 DSG

- Der Auftragsverarbeiter (z.B. ausgelagerte Lohnbuchhaltung) alarmiert und informiert den für die Verarbeitung **Verantwortlichen** unverzüglich nach Feststellung einer Verletzung des Schutzes personenbezogener Daten.

Meldepflicht bei Datensicherheitsverletzungen

Grundlagen

- Der für die Verarbeitung Verantwortliche **benachrichtigt im Anschluss** an die Meldung an die Aufsichtsbehörde **unverzüglich das Datensubjekt**, sofern der Schutz der personenbezogenen Daten, die Privatsphäre oder die Rechte des Datensubjektes durch eine Verletzung beeinträchtigt werden.

  CH: Information des Datensubjekts, wenn es für dieses erforderlich ist oder der Beauftragte dies verlangt, Art. 24 Abs. 4 DSG.

Meldepflicht bei Datensicherheitsverletzungen

Inhalt der Benachrichtigung

Die Benachrichtigung enthält mindestens:

- Eine **Beschreibung** der Art der Verletzung des Schutzes personenbezogener Daten mit Angabe der **Kategorien** und der **Zahl der betroffenen** Datensubjekte, der betroffenen Datenkategorien und der Zahl der betroffenen Datensätze;
- Name und **Kontaktdaten** des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners;
- eine **Beschreibung der wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten;
- gegebenenfalls eine Beschreibung der vorgeschlagenen oder **ergriffenen Massnahmen**.

Informationspflicht (aktiv)
(Art. 19 ff. DSG)

- Um die Transparenz zu gewährleisten, besteht eine **Informationspflicht,** wenn Daten über eine natürliche Person erhoben werden (bei der betroffenen Person selbst oder bei Dritten).
- Diese Pflicht besteht für den Verantwortlichen.

Informationspflicht
(Art. 19 ff. DSG)

- Bisher musste der Inhaber der Datensammlung (Verantwortlicher) gemäss Art. 14 aDSG nur über die Beschaffung (Bearbeitung) von **besonders schützenswerten Personendaten oder Persönlichkeitsprofilen** informieren, neu muss gemäss Art. 19 DSG die betroffene Person über jede **Beschaffung von Personendaten** informiert werden.
- Die Informationspflicht wurde somit auf **alle Personendaten** ausgeweitet, was zu erheblichem Mehraufwand für die Unternehmen führt.

Inhalt der Information

- Mindestens über folgendes muss der Verantwortliche informieren:
  - Identität und Kontaktdaten des Verantwortlichen
  - Bearbeitungszweck
  - (Kategorie) von Empfängerinnen und Empfänger, denen Personendaten bekanntgegeben werden
  - Kategorie der bearbeiteten Personendaten (sofern die Daten nicht bei der betroffenen Person beschafft werden)
  - Bei einer Übermittlung ins Ausland, den Staat oder das internationale Organ und die Garantien, um einen geeigneten Datenschutz zu gewährleisten

Form der Information

- Das Gesetz gibt keine Vorgaben über die Form dieser Information, sie kann beispielsweise in einer Datenschutzerklärung erfolgen.
- Die Information der betroffenen Personen auf einer **Website** wird in der Regel ausreichen.
- Die Person muss die Information erhalten, **ohne zuerst danach fragen zu müssen**.
- **Mehrstufige Erklärung**: In der Praxis empfiehlt es sich, zunächst eine allgemeine Information zu geben. Die betroffene Person hat aber die Möglichkeit, für einzelne Themen konkretere Informationen einzuholen (z.B. über entsprechende Links).
- Gutes Beispiel: Website von Tchibo.

Auskunftsrecht (passiv)
(Art. 25 ff. DSG)

- Jede Person kann vom Verantwortlichen (grundsätzlich kostenlos) Auskunft darüber verlangen:
  - ob Personendaten über sie verarbeitet werden;
  - wenn dies der Fall ist, hat die Person ein Recht auf Auskunft über diese personenbezogenen Daten und auf Zusatzinformationen (Verarbeitungszweck, Kategorien personenbezogener Daten, die Empfänger gegenüber denen die Daten offengelegt worden sind, die Dauer der Speicherung etc.)
- **Empfehlung:** Setzen Sie Prozesse auf, um Auskunftsbegehren (inkl. Löschungsbegehren, Begehren um Einschränkung der Verarbeitung oder Berichtigung der Daten) systematisch erfüllen zu können.

Lösch- und Berichtigungsrecht
(Art. 32 DSG)

- Betroffene können vom Verantwortlichen verlangen, dass ihre Personendaten berichtigt oder (wenn eine Berichtigung nicht möglich ist) gelöscht werden.
- **Ausnahmen** bestehen, wenn eine gesetzliche Vorschrift die Änderung (und somit auch die Löschung) verbietet oder die Personendaten für Archivzwecke im öffentlichen Interesse bearbeitet werden.

Lösch- und Berichtigungsrecht
(Art. 32 DSG)

- Es gibt kein **bedingungsloses** “**Recht auf Vergessenwerden**”. Kann der Verantwortliche einen Rechtfertigungsgrund geltend machen, dann muss er die Daten nicht löschen (z.B. gesetzliche Grundlage oder ein «überwiegendes eigenes Interesse»).
- Daten sind korrekt gelöscht, wenn sie nicht ohne unverhältnismässigen Aufwand wiederhergestellt werden können.

Rechtsfolgen bei einer Verletzung des DSG

- Die Verletzung bestimmter datenschutzrechtlicher Pflichten kann zu einer Geldstrafe von bis zu **CHF 250‘000.00** führen. Bestraft werden – im Gegensatz zur DSGVO – die **Mitarbeitenden**, nicht jedoch das Unternehmen. Die Sanktionierung des Unternehmens ist als **Ausnahmebestimmung** konzipiert (Art. 64 DSG). Bestraft wird nur eine **vorsätzliche** Begehung der Tat auf **Antrag** hin (kein Offizialdelikt).
- Die Verfolgungsverjährung beträgt 5 Jahre (Art. 66 DSG).

Rechtsfolgen bei einer Verletzung des DSG

- Strafbar sind unter anderem
  - die Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten (Art. 60 DSG);
  - die Datenbekanntgabe in ein Empfängerland unter Missachtung der einschlägigen Voraussetzungen (Art. 61 lit. a DSG);
  - die Übertragung der Datenbearbeitung an einen Dritten, ohne dass dieser die Datensicherheit gewährleisten kann (Art. 61 lit. b DSG);
  - die Nichteinhaltung der Mindestanforderungen der Datensicherheit (Art. 61 lit. c DSG);
  - die Missachtung von Verfügungen des EDÖB (Art. 63 DSG).

AUS DER PRAXIS | FÜR DIE PRAXIS

Datenbearbeitung im Arbeitsverhältnis: Folgerungen und Auflösung Beispielsfall

Datenbearbeitung im Arbeitsverhältnis

Folgerungen

Die Definition von Personendaten ist in Art. 4 Abs. 1 DSGVO umfassender als im DSG. Im Zusammenhang mit einem Arbeitsverhältnis sind rasch personenbezogene Daten im Sinne der DSGVO betroffen.

Im Rahmen eines Arbeitsverhältnisses dürfen Daten bearbeitet werden, soweit sie mit dem Vertrag in **notwendigem Zusammenhang** stehen. Dafür braucht es nicht noch einmal eine spezielle Einwilligung des Betroffenen.

Datenbearbeitung im Arbeitsverhältnis

Folgerungen

Es müssen

- die Daten identifiziert werden (**Dateninventar**),
- **Prozesse** definiert werden (Zuständigkeiten und Abläufe) und
- bei drohenden Datenschutzverletzungen muss nach diesen Prozessen **gehandelt** werden (Dokumentation / Meldung an den EDÖB).

Datenbearbeitung im Arbeitsverhältnis

Grenzgänger und die Krux mit der Dienstleistung

Die DSGVO kommt nicht automatisch zur Anwendung, nur weil z.B. ein **Grenzgänger** beschäftigt wird.

Hat dieser kein Schweizer Bankkonto und überweist der Arbeitgeber den Lohn auf ein Bankkonto z.B. in Deutschland, so gibt es jedoch Autoren, welche im Abzug der BVG-Beiträge bereits eine **Dienstleistung** sehen, welche unter den Anwendungsbereich der DSGVO fällt. Auch das Zurverfügungstellen eines Geschäftsfahrzeugs für die Zurücklegung des Arbeitswegs stellt eine solche Dienstleistung dar (Art. 3 Abs. 2 lit. a DSGVO).

Dokumentationspflicht

Bedeutung

- Verfahren mit personenbezogenen Daten dokumentieren
- Risikoabschätzung jedes Verfahrens und Dokumentation
- Gestützt auf Risikoabschätzung technische und organisatorische Massnahmen treffen und dokumentieren
- Implementierung auf Korrektheit prüfen und dokumentieren
- Regelmässige Überprüfung und ggf. Nachführung, Überprüfung der Aktualität dokumentieren

Umsetzung revidiertes DSG

Antworten zum Beispielsfall

Zu denken: “Dumm gelaufen!” reicht rechtlich nicht aus.

Zu treffende Massnahmen:

1. Liegengelassenes Smartphone: Benachrichtigung der Behörde (Risiko für Betroffene)
2. Versand des Rekrutierungsdossiers an den falschen Adressaten: Wenn möglich widerrufen; Dokumentation und Löschung verlangen. Ev. Benachrichtigung der Behörde (Risiko für Betroffene)
3. Hacking des E-Mail-Kontos: Benachrichtigung der Behörde (Risiko für Betroffene und/oder ggf. Datenverlust) und Anzeige gegen unbekannt

Sofortmassnahmen

Lohnender Aufwand hinsichtlich DSGVO und DSG

- ✓ Zentral: **Dateninventar** erstellen (viel Arbeit!): **Wer** bearbeitet **welche Daten** (sach-/personenbezogene) zu **welchem Zweck**?
- ✓ Einwilligungserklärungen dokumentieren
- ✓ Provisorischen Prozess für Datenschutzverletzungen etablieren
- ✓ Provisorischen Prozess für Betroffenrechte (Auskunft, Berichtigung und Löschung) etablieren
- ➢ Planung eines definitiven Verfahrensverzeichnisses: Zuständigkeiten und Abläufe definieren.

Sofortmassnahmen

Lohnender Aufwand hinsichtlich DSGVO und DSG

Hinweis: Zwar ist ein “schriftliches Verzeichnis der Verarbeitungsaktivitäten” gemäss Art. 30 Abs. 5 DSGVO u.a. nicht vorgeschrieben (vgl. Art. 12 Abs. 5 DSG)

- für Unternehmen mit weniger als 250 Mitarbeitenden und
- wenn die Verarbeitung kein Risiko für die Rechte und Freiheiten der Betroffenen birgt.

Doch gerade letzteres ist häufig fraglich, was die 250-MA-Grenze stark relativiert.

AUS DER PRAXIS | FÜR DIE PRAXIS

Fragen & Diskussion

AUS DER PRAXIS | FÜR DIE PRAXIS

Vielen Dank für Ihre Aufmerksamkeit

Kontakt:
Centre Patronal
Markus Hugentobler
Kapellenstrasse 14
3011 Bern
www.centrepatronal.ch