Umsetzungshilfe von aeberli Treuhand AG

Oktober 2022

Anhand der folgenden Fragen und Anweisungen können Sie die neuen Anforderungen aus dem revidierten Datenschutzgesetz in Ihrem Unternehmen umsetzen. Je nachdem, wie Sie die einzelnen Fragen für Ihr Unternehmen beantworten, müssen Sie entweder nichts tun oder Sie können den Anweisungen zu den einzelnen Themen folgen und Ihre Prozesse, internen Richtlinien, Verträge usw. anpassen. Ergänzend zum Leitfaden finden Sie zusätzliche Vorlagen.

Dieser Leitfaden erhebt keinen Anspruch auf Vollständigkeit und stellt keine Rechtsberatung dar. Bitte konsultieren Sie auch das neue Gesetz und die entsprechende Verordnung und lassen Sie sich bei weiteren Unklarheiten durch Datenschutzspezialisten beraten. Weitere Informationen zum Datenschutzgesetz finden Sie auf der Seite des Bundesamts für Justiz:
https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html

Frage	Antwort	Antwort
Haben Sie eine aktuelle **Datenschutzerklärung** für Ihre Website, ihre Verträge, Ihre Auftragsbestätigung usw.?	☐ ja Sie müssen nichts tun	☐ nein ➔ siehe Ziff. 1
Haben Sie interne **Richtlinien** für die Datenbearbeitung (Kundendaten, Lohndaten Ihrer Kunden usw.)?	☐ ja Sie müssen nichts tun	☐ nein ➔ siehe Ziff. 2
Haben Sie ein aktuelles **Verzeichnis** aller Datenbearbeitungen in Ihrem Unternehmen?	☐ ja Sie müssen nichts tun	☐ nein ➔ siehe Ziff. 3
Haben Sie eine Vorgehensweise für die rechtzeitige Beantwortung von **Auskunftsbegehren** (z.B. Ersuchen um Auskunft oder Löschung von Daten)?	☐ ja Sie müssen nichts tun	☐ nein ➔ siehe Ziff. 4
Haben Sie einen Prozess für die rechtzeitige Meldung einer **Verletzungen** des Datenschutzes (wer meldet wem was wie rasch)?	☐ ja Sie müssen nichts tun	☐ nein ➔ siehe Ziff. 5
Haben Sie **Subunternehmern** bzw. deren Verträge geprüft, ob die Sicherheit der Personendaten gewährleistet ist, ob diese die Personendaten nur so bearbeiten, wie sie selbst sowie vor Beauftragung eines Subsubunternehmers Ihre Einwilligung eingeholt, und entsprechende Klauseln hinzugefügt?	☐ ja Sie müssen nichts tun	☐ nein ➔ siehe Ziff. 6
Haben Sie einen Prozess zur **Löschung** oder Anonymisierung von allen personenbezogenen Daten einer betroffenen Person?	☐ ja Sie müssen nichts tun	☐ nein ➔ siehe Ziff. 7
Werden Ihre Daten ausschliesslich in der **Schweiz gespeichert**? Falls nein, haben Sie geprüft, ob diese Länder auf der Liste des Bundesrates stehen und allfällige weitere Massnahmen ergriffen?	☐ ja Sie müssen nichts tun	☐ nein ➔ siehe Ziff. 8
Haben Sie Ihre Prozesse und **IT Infrastruktur überprüfen** lassen, ob sie einen angemessenen Sicherheitsstandard durch zeitgemässe technische und organisatorische Massnahmen erfüllen (z.B. Passwortrichtlinien, hat ihr IT Partner die neuesten Updates, Firmwares etc. installiert)?	☐ ja Sie müssen nichts tun	☐ nein ➔ siehe Ziff. 9
Übermitteln Sie **besonders schützenswerte Personendaten** unverschlüsselt?	☐ nein Sie müssen nichts tun	☐ ja ➔ siehe Ziff. 10
Bieten Sie **Datenherausgabe** in einem gängigen elektronischen Format an?	☐ ja Sie müssen nichts tun	☐ nein ➔ siehe Ziff. 11
Ist Ihnen der Begriff **Datenschutz-Folgeabschätzung** bekannt und führen Sie solche im Bedarfsfall durch?	☐ ja Sie müssen nichts tun	☐ nein ➔ siehe Ziff. 12

1. Datenschutzerklärung

Brauchen Sie eine Datenschutzerklärung auf Ihrer Website?
Brauchen Sie eine Datenschutzerklärung für Ihre Verträge mit Ihren Kunden?

Da Sie als Unternehmen fast immer Personendaten beschaffen, müssen Sie informieren, zu welchem Zweck Sie Personendaten bearbeiten, wem Sie sie bekannt geben (nicht einzelne Namen, aber Kategorien von Empfängern, z.B. «Gruppengesellschaften», «Partnern», «IT-Dienstleistern», «Behörden» usw.), ob und ggf. welche Daten von Dritten beschafft werden (d.h. nicht vom Betroffenen selbst) und ob Daten ins Ausland gehen. Die Formulierung einer Datenschutzerklärung – oder mehrerer Erklärungen – ist deshalb eine Hauptaufgabe bei der Vorbereitung auf das neue Gesetz.

Bei der Erfüllung der Informationspflicht stellt sich sehr häufig die Frage, ob es genügt, aus einer Drucksache – z.B. AGB oder einer schriftlichen Mitteilung – auf eine Datenschutzerklärung im Internet zu verweisen. Wir gehen davon aus, dass eine Publikation im Internet ausreichend ist, wenn Sie zumindest auf die Internetseite hinweisen.[1]

Der Betroffene (z.B. Ihr Kunde) kann auch durch Einwilligungen auf Datenbearbeitungen einwirken, indem er Bearbeitungen legitimiert, die sonst unzulässig wären. Das ist aber nur ausnahmsweise erforderlich, denn das DSG und das revDSG verlangen keine besondere Rechtsgrundlage. Es genügt, die Bearbeitungsgrundsätze einzuhalten. Eine Einwilligung ist deshalb nur erforderlich, wenn eine Bearbeitung den erlaubten Rahmen überschreitet, bspw. wenn besonders schützenswerte Personendaten an Dritte weitergegeben werden.

Sie können Ihrem Kunden die Datenschutzerklärung bei Vertragsabschluss zustellen oder ihn auf Ihre Datenschutzerklärung auf Ihrer Website hinweisen. Sie können auch unterschiedliche Datenschutzerklärungen einsetzen, beispielsweise eine Version nur für Ihre Website-Besucher.

Braucht es eine Datenschutzerklärung auf Ihrer Website? Selbst wenn Sie auf Ihrer Website keinerlei Daten sammeln und die Website-Besucher keine Daten eingeben können, empfehlen wir eine Datenschutzerklärung auf Ihrer Website zu publizieren. Falls keine Daten gesammelt werden, könnte dies in der Datenschutzerklärung erwähnt werden. Häufig verfügen Websites aber mindestens über ein Kontaktformular. Der Zweck ist die Kontaktaufnahme. Dafür wird beispielsweise ein Formular-Dienst aus den USA eingebunden. Wenn jemand das Formular ausfüllt, werden die Angaben bei diesem Formular-Dienst gespeichert und Sie erhalten die Angaben ausserdem per E-Mail. Die Angaben umfassen Namen und E-Mail-Adressen sowie Mitteilungen. Dazu kommen Datum und Zeit sowie IP-Adressen als Metadaten. Und schon haben Sie eine Sammlung von Daten und bearbeiten solche. Sie müssen die Website Besucher darüber informieren, am besten in einer Datenschutzerklärung.

Die Datenschutzerklärung muss insbesondere folgende Angaben enthalten:

- Wer ist für die Datenbearbeitung verantwortlich und wie kann der Kontakt erfolgen?[2]
- Für welchen Zweck oder für welche Zwecke werden die Personendaten bearbeitet?
- Wer sind allfällige Empfänger der bearbeiteten Personendaten und in welchen Ländern/Regionen befinden sich diese?
- Wie wird ein allfälliger Daten-Export abgesichert?
- Welche Rechte haben die betroffenen Personen im Zusammenhang mit dem Datenschutz?

[1] Siehe Fachartikel von Dr. David Vasella „Das neue Datenschutzgesetz und seine Umsetzung", erschienen im TREX, Ausgabe 5/21
[2] Eine allgemeine E-Mail-Adresse ist ausreichend: datenschutz@unternehmen.ch

2. Richtlinien für die Datenbearbeitung

Wir empfehlen, Richtlinien für die Datenbearbeitung innerhalb des Unternehmens zu erstellen.

Folgende Punkte sollten darin enthalten sein:

- Wer hat Zugriff* auf welche Daten
- Wer darf welche Daten bearbeiten
- Wo müssen die Daten gespeichert werden
- Wie/wann werden Daten wieder gelöscht
- Welche Daten dürfen nur verschlüsselt verschickt werden
- Welche Regeln gelten mit dem Umgang mit Daten (Verwendung von Passwörtern, Clean Desk usw.)
- Spezielle Regelungen

Die Dokumentation der Prozesse ist hilfreich für behördliche Anfragen oder allfälligen Rechtsverfahren.

*Zugriffsrechte müssen konsequent in allen Softwarelösungen und Ordnerstrukturen aktuell gehalten werden. Insbesondere bei Personalwechsel muss die Aktualisierung im entsprechenden HR-Prozess vorgesehen sein.

3. Verzeichnis aller Datenbearbeitungen

Unternehmen mit weniger als 250 Beschäftigten müssen kein Verzeichnis führen, ausser es besteht ein hohes Risiko für die betroffenen Personen. Obwohl bei vielen KMUs in der Regel kein hohes Risiko für die betroffenen Personen (Kunden und Mitarbeitende) bestehen dürfte, empfehlen wir, in jedem Fall ein Verzeichnis zu führen, denn diese Übersicht hilft bei diversen anderen Vorgaben des revDSG. Eine einfache Excel- oder Wordliste genügt. Wir stellen Ihnen gerne eine Mustervorlage zur Verfügung.

Beispiel:

Bearbeitungstätigkeiten — Blatt 1

Nr.	gemeinsam Verant-wortliche	Zweck	Kategorien betroffener Personen	Kategorien personenbezogener Daten	Empfänger	Übermittlung in Drittstaaten	Löschfristen	Techn. u. organis. Massnahmen	Datum der letzten Änderung
01	-	Lohn- und Gehaltsbrech-nung	Mitarbeitende	Stamm- und Vertragsdaten, Bankverbindungsdaten, Sozialversicherungsdaten, Abrechnungsdaten bzw. Lohndaten	Personalabteil ung, externes Lohnverrechnu ngsbüro, Sozialversicher ung	nein	nach Ablauf gesetzlicher Fristen bzw. Verjährung möglicher rechtlicher Ansprüche (genau zu bezeichnen)	Schutzniveau erhöht - Massnahmen gem. Sicherheits-konzept: z.B. Personalabteilung gesonderter Zutrittsbereich; Zugriffskontrolle Daten	1.4.2022
02	-	Arbeitszeit-erfassung	Mitarbeitende	Stamm- und Vertragsdaten, Arbeitszeiten, Krankheiten, Ferienbezug, sonstige Abwesenheiten	Personalabteil ung	nein	nach Ablauf gesetzlicher Fristen bzw. Verjährung möglicher rechtlicher Ansprüche (genau zu bezeichnen)	Schutzniveau erhöht - Massnahmen gemäss Sicherheitskonzept: Zugriffskontrolle Daten	3.5.2022
03	-	Reise-management	Mitarbeitende	Stammdaten, Buchungsdaten, Legitimationsdaten (Kreditkartennr.)	SBB, Swiss oder andere Fluglinien, Reisebüro	ja, bei Reisen ins Ausland an ausländische Fluglinien oder für Visa	nach Ablauf von handels- oder steuerrechtlichen Aufbewahrungs-pflichten (genau zu bezeichnen)	Schutzniveau normal – keine besonderen Massnahmen erforderlich	1.4.2022
04	-	Kunden-betreuung	aktive und ehemalige Kunden	Stamm-, Vertrags- und Leistungsdaten, Abrechnungsdaten, Korrespondenz, etc.	Finanzbuchhal tung, Vertrieb	nein	nach Ablauf von handels- oder steuerrechtlichen Aufbewahrungs-pflichten (genau zu bezeichnen)	siehe oben	4.5.2022
05		Beschaffung	Lieferanten (wenn natürliche Person)	betriebliche Kontaktdaten, Informationen über Kenntnisse und Fähigkeiten	Abteilung Einkauf intern	nein	nach Ablauf von handels- oder steuerrechtlichen Aufbewahrungs-pflichten (genau zu bezeichnen)	siehe oben	4.5.2022

4. Auskunftsbegehren

Betroffene Personen (Kunden, Websitebesucher usw.) haben zahlreiche Rechte im Zusammenhang mit der Bearbeitung ihrer Daten. Sie können ein Auskunfts- oder Löschbegehren stellen. Solche Begehren müssen innerhalb kurzer Frist (in der Regel innerhalb 30 Tagen) beantwortet werden. Legen Sie fest, wer für die Beantwortung der Begehren zuständig ist. Das Verzeichnis aller Datenbearbeitungen (Ziff. 3) hilft, die entsprechenden Angaben zusammenzustellen.

Auch wenn nicht davon auszugehen ist, dass viele Ihrer Kunden ein Auskunftsbegehren stellen werden, ist dennoch zu empfehlen, einen entsprechenden Prozess inkl. Vorlage vorzubereiten.

Gerne stellen wir Ihnen eine Mustervorlage eines Antwortschreibens zur Verfügung.

Ihre Adresse...

Ihre Adresse

Empfänger-Adresse

Ort, Datum wählen

Erteilung der Auskunft nach Art. 25 DSG

Anrede eingeben

In Beantwortung Ihres Antrages auf Auskunft nach Art 25 DSG vom Datum wählen kommen wir, nach ausreichender Prüfung Ihrer Identität, hiermit innerhalb der gesetzlichen Frist von einem Monat Ihrem Antrag nach.

1. Zu Ihrer Person haben wir folgende Daten gespeichert:
Name:
Vorname:
Anschrift:
Telefon:
E-Mail:
.....
.....
.....

Eine Kopie der relevanten Datenbearbeitungen finden Sie in der Beilage.

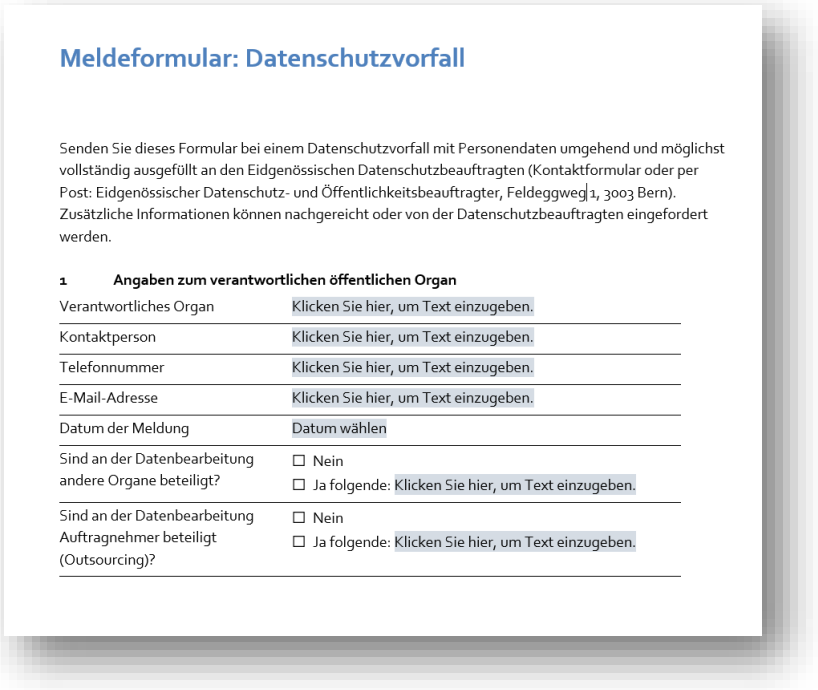
2. Verarbeitungszwecke:
Wir nutzen Ihre oben stehenden Daten ausschliesslich zum Zwecke der [Verarbeitungszweck eintragen].

3. Datenkategorien:
Wir bearbeiten folgende Kategorien: [Info Einfügen, Beispiel: Adress- und Kontaktdaten].

5. Prozess Meldung Verletzung Datenschutzes

Eine Datenschutzverletzung liegt vor, wenn Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Solche Meldungen von Verletzungen, die für die Betroffenen zu einem hohen Beeinträchtigungsrisiko ihrer Persönlichkeit oder ihrer Grundrechte führen, müssen so rasch wie möglich (in der EU innerhalb von 72 Stunden) an den Eidgenössischen Datenschutzbeauftragten EDÖB gemeldet werden. Bei geringem Risiko kann die Meldung freiwillig erfolgen. Zum Schutz der betroffenen Person, sollte auch die betroffene Person bei hohem Beeinträchtigungsrisiko informiert werden. Auftragsbearbeiter (also möglicherweis auch externe Dienstleister) müssen alle Datensicherheitsverletzungen dem Verantwortlichen ohne Verzug melden. Um eine Verletzung des Datenschutzes umgehend entdecken zu können sind organisatorische und technische Massnahmen notwendig. Ein Verzeichnis aller Datenbearbeitungen hilft mögliche Datenschutzverletzungen zu entdecken (Ziff. 3).

Gerne stellen wir Ihnen eine Mustervorlage einer Meldung an den EDÖB zur Verfügung.



Meldeformular: Datenschutzvorfall

Senden Sie dieses Formular bei einem Datenschutzvorfall mit Personendaten umgehend und möglichst vollständig ausgefüllt an den Eidgenössischen Datenschutzbeauftragten (Kontaktformular oder per Post: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Feldeggweg 1, 3003 Bern). Zusätzliche Informationen können nachgereicht oder von der Datenschutzbeauftragten eingefordert werden.

1 Angaben zum verantwortlichen öffentlichen Organ

Verantwortliches Organ	Klicken Sie hier, um Text einzugeben.
Kontaktperson	Klicken Sie hier, um Text einzugeben.
Telefonnummer	Klicken Sie hier, um Text einzugeben.
E-Mail-Adresse	Klicken Sie hier, um Text einzugeben.
Datum der Meldung	Datum wählen
Sind an der Datenbearbeitung andere Organe beteiligt?	☐ Nein ☐ Ja folgende: Klicken Sie hier, um Text einzugeben.
Sind an der Datenbearbeitung Auftragnehmer beteiligt (Outsourcing)?	☐ Nein ☐ Ja folgende: Klicken Sie hier, um Text einzugeben.

6. Verträge mit Subunternehmen / Dienstleister überprüfen

Für viele Funktionen werden Dienste von Dritten eingesetzt, zum Beispiel für den E-Mail- und Newsletter-Versand, Buchhaltungssoftware in der Cloud, Software-as-a-Service-Anbieter oder für Video-Konferenzen. Vermutlich arbeiten auch Sie mit Dienstleistern zusammen.

Die Auslagerung der Datenbearbeitung an Subunternehmen ist möglich, wenn folgende Voraussetzungen erfüllt sind:

- Es werden keine Geheimhaltungspflichten verletzt
- Der Auftragsbearbeiter darf die Daten nur so bearbeiten, wie es der Auftraggeber selbst darf. Zweckänderung sind nicht erlaubt
- Der Auftragsbearbeiter muss in der Lage sein, die Datensicherheit zu gewährleisten
- Die Unter-Auftragsbearbeitung darf nur mit vorgängiger Genehmigung erfolgen

Überprüfen Sie die Verträge mit Subunternehmern darauf, dass die Sicherheit der Daten gewährleistet ist, und fügen Sie entsprechende Klauseln hinzu, wenn nötig (insbesondere bezüglich der Meldung jeglicher Verletzungen des Datenschutzes). Betreffend Klauseln siehe auch Ziff. 8.

Wir empfehlen auch die Aufnahme einer Meldepflicht bei Datenschutzverletzungen und eine Genehmigungspflicht bei der Weitergabe an Unter-Auftragnehmer.

7. Wann müssen Daten gelöscht werden?

Personendaten, die nicht mehr benötigt werden und für deren Bearbeitung kein Rechtfertigungsgrund nachgewiesen werden kann, müssen vom Unternehmen gelöscht werden. Daten sind korrekt gelöscht, wenn sie nicht ohne unverhältnismässigen Aufwand wiederhergestellt werden können.

Überprüfen Sie anhand dem Verzeichnis Ihrer Datenbearbeitungen (Ziff. 3), ob Sie bei allen Datenbearbeitungen einen Lösch-Prozess eingeplant haben.

8. Datenübermittlung ins Ausland

Die meisten Cloud- und Software-as-a-Service-Anbieter (Buchhaltungssoftware, E-Mail Newsletters, CRM usw.) haben Server ausserhalb der Schweiz. Personendaten dürfen ins Ausland bekanntgegeben werden, wenn die Gesetzgebung des betreffenden Staates (oder das internationale Organ) einen angemessenen Schutz gewährleistet. Der EDÖB bzw. künftig nach revDSG der Bundesrat führt eine Liste der «sicherer Drittstaaten», siehe Statenliste hier. Bei «unsichere Drittstaaten» z.B. USA sind zusätzliche Vertragsklauseln sowie allfällige weitere Sicherheitsmassnahmen notwendig.

Beim Daten-Export in die USA (also auch dem Speichern von Personendaten auf Servern in den USA), zum Beispiel durch die Nutzung eines Internet-Dienstes in den USA, kann ein angemessener Datenschutz mit sogenannten Standardvertragsklauseln, englisch Standard Contractual Clauses (SCC), sowie allfälligen weiteren Sicherheitsmassnahmen (Anonymisierung, Verschlüsselung etc.) gewährleistet werden. Sollten Sie Daten in die USA exportieren bzw. US-Dienstleister nutzen, müssen Sie prüfen, ob auf solche Standardvertragsklauseln verwiesen wird bzw. diese einschliesst. Häufig sind sie Bestandteil der AGB oder AVV (Auftragsverarbeitungsvertrag). Falls nicht, müssen Sie selbst veranlassen, dass diese Klauseln eingeschlossen werden. Auch den Einsatz allfälliger weiterer Sicherheitsmassnahmen müssen Sie im Rahmen einer Risikoabschätzung sowie ggf. einer Datenschutz-Folgenabschätzung (DSFA) beurteilen.

9. IT Infrastruktur

Je nach Risiko der Daten müssen entsprechende technische und organisatorische Massnahmen ergriffen werden. Personendaten aus der Personalabteilung sind besonders heikel und sollten mit Vorsicht bearbeitet werden. Treuhänder speichern auch sensitive Kundendaten und sollten daher der Datensicherheit einen hohen Stellenwert einräumen.

Um die Datensicherheit zu gewährleisten, empfehlen wir, die IT Infrastruktur durch einen externen Spezialisten prüfen zu lassen. Dieser testet, ob

- organisatorische Massnahmen vorhanden sind (z.B. interne Richtlinien, Passwortrichtlinien, Passwortmanager, Schulung/Sensibilisierung der Mitarbeitenden usw.)
- alle Software auf dem neuesten Stand sind mit allen sicherheitsrelevanten Updates
- ob alle Geräte mit modernen Virenscanner geschützt sind
- ob aktuelle Firmware im Einsatz sind
- ob Firewall korrekt konfiguriert ist
- ob Daten Back-up korrekt durchgeführt werden.

Auch wenn Sie einen externen IT Partner haben, können Sie nicht sicher sein, dass alle oben erwähnten Punkte erfüllt sind. Zudem gehört «Betrug» zu den häufigsten Cybervorfällen und die Schwachstelle ist der Mensch (Passwörter). Hier setzen organisatorische Massnahmen an und weniger technische.

10. Besonders schützenswerte Personendaten

Besonders schützenswerte Personendaten sollte man auch besonders schützen und auch immer nur verschlüsselt übermitteln. Unter diese fallen unter anderem:

- personenbezogene Daten, aus denen rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen einer Person hervorgehen
- Gewerkschaftszugehörigkeit
- genetische Daten, biometrische Daten, die ausschließlich zur eindeutigen Identifizierung einer natürlichen Person verarbeitet werden
- Gesundheitsdaten
- Daten zum Sexualleben oder zur sexuellen Orientierung einer Person.
- Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen
- Daten über Massnahmen der sozialen Hilfe

Lohndaten gehören nicht zu besonders schützenswerte Personendaten. Eine Bestätigung, dass diese Daten aber unverschlüsselt verschickt werden dürfen, ist dennoch empfehlenswert.

11. Datenportabilität

Mit dem Recht auf Datenherausgabe hat eine betroffene Person die Möglichkeit, ihre Personendaten, welche sie einem privaten Verantwortlichen bekanntgegeben hat, in einem gängigen elektronischen Format heraus zu verlangen oder einem Dritten übertragen zu lassen. Vorausgesetzt ist, dass die Daten automatisiert und mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit einem Vertrag bearbeitet wird.

Dieses Recht, das dem Kartellrecht wohl nähersteht als dem Datenschutzrecht, soll im Interesse des Wettbewerbs den Anbieterwechsel erleichtern. Welche Bedeutung es in der Praxis erlangt, wird sich weisen.

12. Datenschutz-Folgenabschätzung

Unternehmen müssen Risiken durch seine Bearbeitung von Personendaten in jedem Fall einschätzen. Oft genügt eine intuitive Risikoeinschätzung. Bestimmte Bearbeitungen sind aber heikler. Hier sind vertiefte Überlegungen notwendig. Wenn eine Bearbeitung voraussichtlich hohe Risiken mit sich bringt, verlangt das revDSG, dass der Verantwortliche Risiken im Rahmen einer Datenschutz-Folgenabschätzung (DSFA) beurteilt und dokumentiert.

Ob hohe Risiken vorliegen, ist nicht immer einfach zu beurteilen. Eine DSFA sollte aber jedenfalls dann durchgeführt werden, wenn besonders schützenswerte Personendaten in grösserem Umfang bearbeitet werden. Davon ist aber nicht schon dann die Rede, wenn Mitarbeiterdaten bearbeitet werden, auch wenn diese besonders schützenswerte Personendaten enthalten.