Merkblatt Datenschutzpflichten

RECHT VERNETZT

ipeakinfosystems

Unsere Kunden stellen im Umgang mit ihren persönlichen Daten immer höhere Ansprüche an unsere Unternehmen und müssen daher besonders geschützt werden.

Das im September 23 in Kraft tretende neue DSG zielt darauf ab, die gesetzlichen Anforderungen an die jüngsten technologischen Entwicklungen anzupassen und gleichzeitig das **Schutzniveau für den Einzelnen zu erhöhen**. Im Grundsatz geht es darum, dass jede Verarbeitung von Daten die sich auf eine identifizierte oder direkt bzw. indirekt identifizierbare Person bezieht, verhältnismässig ist und nicht missbraucht werden kann.

Durch diese Stärkung und Einführung neuer Rechte für unsere Kunden und Mitarbeitenden (Rechte im Bezug auf Zugang, Löschung, Übertragbarkeit persönlicher Daten usw.), schafft dieses Gesetz auch **neue Verpflichtungen für Unternehmen**. Diese haben nicht nur die Pflicht auf Anfrage von Privatpersonen hin zu informieren und zu reagieren, sondern müssen Datenschutz-verletzungen aktiv melden.

Das heisst, sobald Sie Daten bearbeiten, sind Sie verpflichtet das DSG einzuhalten. Datenbearbeitung beginnt bereits bei der Erfassung von Daten. Jegliche Datenbearbeitungsschritte, die nachfolgend beispielhaft aufgezeichnet sind, müssen Datenschutz-konform sein.

Aufgrund der Kürze des Merkblattes wird auf gendergerechte Formulierung verzichtet. Mit der männlichen Bezeichnung sind jeweils alle Geschlechterrollen gemeint.

Gesetzliche Anforderungen

Um sich bestmöglich auf dieses neue regulatorische Regime vorzubereiten, müssen KMU einen ganzheitlichen Ansatz verfolgen:

RISIKEN EINSCHÄTZEN

Unternehmen, die grosse Mengen an Daten verarbeiten, sind einem höheren Risiko ausgesetzt. Es ist für sie daher wichtig, alle **personenbezogenen Daten** (Kunden, Lieferanten, Mitarbeitende usw.) und sogenannte «sensible Daten» (Religion, Gesundheit, Genetik usw.) welche in IT-Systemen, Datenbanken und Produkten von ipeak und sämtlichen anderen IT-Dienstleistern erfasst werden, korrekt zu bearbeiten und zu sichern.

ORGANISIEREN UND ABSICHERN

Die **Optimierung von Datenschutzprozessen und der IT-Sicherheit** können helfen, sich vor Datenschutzverletzungen, -verlusten, -lecks zu schützen und auf Anfragen von Einzelpersonen richtig zu reagieren.

BEWUSSTSEIN SCHÄRFEN

Alle Ebenen eines Unternehmens, vom Auszubildenden bis zum Geschäftsführer, sollten beim Datenschutz einbezogen, **geschult und sensibilisiert** werden. Bei vorsätzlichem Fehlverhalten können einzelne Personen sanktioniert werden.

Dabei sollen vor allem nachfolgende Prinzipien im Fokus behalten werden:

- ❖ Einwilligung
- ❖ Transparenz
- ❖ Verhältnismässigkeit
- ❖ Richtigkeit

Was sind die wichtigsten konkreten Pflichten für Unternehmen? (1)

Ein pragmatischer Umsetzungsplan beinhaltet mindestens die Einhaltung folgender Prinzipien:

- **Transparenz und Information**

Sobald Sie Daten bearbeiten, müssen Sie die betroffene Person über den ganzen Prozess der Datenbearbeitung(en) zwingend informieren. Dazu erstellen Sie eine **Datenschutzerklärung** (DSE), welche Sie bei Bedarf aktualisieren. Auf der Unternehmenswebsite sowie auf jeglicher Applikation, wo Daten erfasst werden können, ist die DSE zu verlinken.

- **Umfassende Bestandsaufnahme**

Sie müssen bestimmte Informationspflichten erfüllen, d.h. Sie müssen bei der Beschaffung von Personendaten unter anderem über die Identität des Verantwortlichen, den Bearbeitungszweck, allfällige Datenempfänger informieren. Zudem müssen Sie in der Lage sein, die Betroffenenrechten zu erfüllen, etwa einer betroffenen Person Auskünfte zur Bearbeitung ihrer Personendaten zu erteilen. Das alles setzt voraus, dass Sie wissen, welche Personendaten zu welchen Zwecken bearbeitet werden, ob die Daten in andere Länder und an weitere Personen transferiert werden etc.. Um dies sicherzustellen, sollen Sie zunächst eine Bestandsaufnahme aller Datenbearbeitungen durchführen.

- **Datenschutz-Folgeabschätzung**

Abschätzung der Risiken: Je grösser das Volumen der von einem Unternehmen bearbeiteten Personendaten und/oder je sensibler die Personendaten sind, desto höher sind die Anforderungen an die Datenschutz-Compliance bzw. desto grösser sind die potentiellen Sanktionen und Reputationsschäden bei einem Verstoss. Deshalb gilt hier die Verpflichtung, in bestimmten Fällen eine Folgenabschätzung zum Schutz der Personendaten durchzuführen.

Was sind die wichtigsten konkreten Pflichten für Unternehmen? (2)

- **Privacy by design und by default**

Durch den Einsatz von Technik und datenschutzfreundlichen Voreinstellungen stellen Sie sicher, dass die Bearbeitungsgrundsätze eingehalten werden und sich die Datenbearbeitungen auf das für den Verwendungszweck nötige Mindestmass beschränken.

- **IT-Sicherheit**

Sie müssen sicherstellen, dass die Sicherheit ihrer IT-Systeme und Software-Anwendungen den Vorgaben des neuen Gesetzes entspricht. Dazu gehören insbesondere technische und organisatorische Massnahmen zur Verhinderung von Cyberattacken, Datendiebstahl und anderweitigem Datenverlust.

- **Meldepflicht**

Im Falle einer Datenschutzverletzung müssen Sie diese dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sowie der betroffenen Person umgehend melden.

- **Ernennung von Datenschutzbeauftragter Person**

Sie definieren für Ihre Unternehmung eine Datenschutzbeauftragte Person.

- **Sensibilisierung & Schulung**

Sie müssen alle Ihre Mitarbeitenden, vom Lernenden bis zum Geschäftsführer, regelmässig zum Thema Datenschutz schulen und sensibilisieren.

Alle Mitarbeitenden bearbeiten regelmässig Personendaten und tragen hierfür die Verantwortung.

Beispiel: Die Empfangsabteilung führt ein Register der Besucher eines Unternehmens. Indem Vor- und Nachnamen von Personen, die das Unternehmen besuchen, erfasst und archiviert werden, bearbeiten sie bereits Personendaten.

Was sind die wichtigsten konkreten Pflichten für Unternehmen? (3)

- **Interne Organisation und Abläufe**

Sie müssen auf Betroffenenanfragen (z.B. Auskunfts- oder Löschbegehren eines Kunden) oder auf eine Verletzung der Datensicherheit („Datenpannen“), bei denen Personendaten verloren gehen, gestohlen oder missbraucht werden, gesetzeskonform reagieren können.

Dazu müssen klare interne Prozesse festgelegt werden. Diese Prozesse sollten je nach Vorfall insbesondere definieren, welcher Mitarbeiter (inkl. Vertretung) welche Massnahmen innert welcher Frist treffen muss.

Beispiel: Verletzung der Datensicherheit

Erarbeiten Sie einen Überblick von Fallbeispielen bzw. Kriterien, nach denen zu beurteilen ist, ob ein Vorfall einer Behörde gemeldet werden muss. Dazu gehören Ausführungen, welcher Mitarbeiter diese Meldung innert welcher First und in welcher Form an welche Behörde vornehmen muss (Checklisten).

- **Erstellung und Führung eines Verzeichnisses der Bearbeitungstätigkeiten**

Sie als Daten-Verantwortlicher als auch ihr Auftragsbearbeiter, müssen je ein Verzeichnis über ihre Bearbeitungstätigkeiten führen. Diese Pflicht gilt grundsätzlich für alle Unternehmen. Der Bundesrat kann jedoch Ausnahmen vorsehen für Unternehmen mit weniger als 250 Mitarbeitern. Das Erstellen solcher Verzeichnisse setzt voraus, dass sämtliche Bearbeitungen von Personendaten innerhalb eines Unternehmens identifiziert und systematisch zusammengetragen werden. Gerade in Fällen, wo noch keine entsprechenden Verzeichnisse geführt werden und viele verschiedene Bearbeitungen durchgeführt werden, ist dieser Prozess mit einem beträchtlichen Aufwand verbunden und sollte daher frühzeitig angegangen werden.

Was sind die wichtigsten konkreten Pflichten für Unternehmen? (4)

- **Überprüfung von Verträgen**

Prüfen Sie Ihre Verträge mit Kunden, Lieferanten und Dienstleistern sowie Arbeitnehmern mit Blick auf die Neuerungen und passen Sie diese ggf. an. Eine rasche Umsetzung ist auch deshalb angezeigt, weil damit gerechnet werden muss, dass viele Vertragspartner in den kommenden Monaten Verträge bzw. Vertragsanpassungen verlangen werden, um ihrerseits Datenschutz-Compliance sicherzustellen.

- **Informiert bleiben**

Um sich dem Thema Datenschutz-Compliance bewusst zu werden, müssen Sie in der Lage sein, die konkreten Auswirkungen des neuen Gesetzes auf die eigenen Bearbeitungsprozesse zu verstehen. Informieren Sie sich auf den Internetseiten der Datenschutzbehörde (EDÖB), auf einschlägigen Blogs, in Fachzeitschriften und nehmen Sie an den verschiedenen Schulungen teil. Wenn Sie diesen Aufwand in Ihrer Unternehmung nicht leisten können, prüfen Sie die Zusammenarbeit mit einem externen Datenschutzexperten.

ipeakinfosystems

Wie setzen Sie diese Punkte konkret bei der Verwendung von ipeak-Produkten um?

- **Informationssysteme: Displays und Applikationen**

Stellen Sie bei der Verwendung der digitalen Kommunikationslösungen (Mobile Webapp) und der multimedialen Installationen (Touchscreen, Anzeigen) sicher, dass Sie die Menge von personalisierten Daten oder Fotomaterial von Personen möglichst geringhalten.

Was ist zu tun wenn Sie bei Anzeigen auf dem Touch- oder Infoscreen bei Informationen wie „Heute hat Geburtstag“, „Neu im Team“ oder „Wer wohnt wo“ Personendaten publizieren?

Wenn Sie personalisierte Daten Ihrer Mitarbeitenden oder Bewohnern (Namen, Geburtsdatum, Telefonnummer etc.) oder Fotos einzelner Personen auf Screens oder mobilen Webapps publizieren, benötigen Sie die Einwilligung der betroffenen Person.

- **Erfassung von Daten**

Sobald ein Nutzer über eine Applikation, Touchscreen oder in der mobilen App personalisierte Daten eingibt (bspw. für die Erstellung eines Logins mit Name, E-Mail-Adresse etc.) muss dieser Person im Sinne der Transparenz und Information aufgezeigt werden, was mit seinen Daten passiert.

Diese Informationen dokumentieren Sie in einer Datenschutzerklärung. Diese Datenschutzerklärung muss auf der Applikation abrufbar sein und muss vor dem Absenden der personalisierten Daten akzeptiert werden*.

Beispiel:

□ *Mit dem Absenden stimme ich der in der Datenschutzerklärung umschriebenen Bearbeitung meiner Personendaten zu.*

*Bitte kontaktieren Sie uns für eine Aufschaltung Ihrer Datenschutzerklärung.

Einstieg: 12 Fragen zum Selbsttest

- Sind bei Ihnen alle Datensammlungen und Bearbeitungsverfahren sauber dokumentiert?
- Haben Sie überall dort, wo Daten bearbeitet werden, eine für den Datenschutz verantwortliche Person mit entsprechendem Know-how und Ressourcen?
- Sind alle grenzüberschreitenden Datenflüsse in Länder ohne angemessenen Datenschutz vertraglich oder analog abgesichert, auch intern?
- Sind alle internen und externen Auftragsdatenbearbeitungen vertraglich geregelt?
- Ist jede relevante Datenbearbeitung durch eine passende Weisung geregelt?
- Sind Massnahmen zur Sicherstellung der Datensicherheit im Betrieb auf dem Stand der Technik?
- Sind alle Mitarbeiter in Sachen Datenschutz ausgebildet und sensibilisiert?
- Wird die Einhaltung der erforderlichen Datensicherheit und der Bestimmungen des Datenschutzes intern oder von extern überprüft?
- Sind alle nötigen Meldungen und Registrierungen erfolgt und alle Bewilligungen eingeholt?
- Sind alle Datenbearbeitungen, wo erforderlich, transparent kommuniziert?
- Verfügen alle Verträge mit Dritten über angemessene Datenschutzklauseln?
- Sind alle Prozesse zur Sicherstellung des Datenschutzes definiert, insbesondere bezüglich der Rechte der betroffenen Personen, bezüglich neuer Projekte, bezüglich Verträge mit Providern?

Impressum

- Dieses Merkblatt wurde von der RECHT VERNETZT GmbH für die ipeak Infosystems GmbH erstellt.
- Bei technischen Fragen zu Ihren Anwendungen wenden Sie sich an ipeak Infosystems.
- Die Datenschutzerklärung der ipeak Infosystems GmbH finden Sie hier: https://ipeak.ch/uber-uns/datenschutz/
- Für allfällige rechtliche Fragen und zu Fragen zum neuen Datenschutzgesetz steht Ihnen die RECHT VERNETZT GmbH gerne zur Verfügung. bettina.huebscher@rechtvernetzt.clubdesk.com