TREUHAND | SUISSE

Schweizerischer Treuhänderverband

Datenschutz im Treuhandbereich

Eine Publikation, Leitfaden von:

INSTITUT TREUHAND UND RECHT

INSTITUT TREUHAND 4.0

Bern, August 2021

1. Das Wichtigste in Kürze

Das Parlament hat das totalrevidierte Schweizer Datenschutzgesetz (DSG) am 25.09.2020 angenommen und nach der Erarbeitung der entsprechenden Verordnung ist mit der Inkrafttretung des Gesetzes im Jahr 2023 zu rechnen.

Im neuen Schweizer Datenschutzgesetz werden folgende Punkte genauer geregelt: besonders schützenswerte Personendaten, Profiling (maschinelle Auswertung von Personendaten), erweiterte Informationspflicht, Rechte von Betroffenen, Strafbestimmungen.

Dieser Leitfaden dient als Auflistung der einzelnen Punkte, die Sie in Bezug auf das neue Datenschutzgesetz beachten müssen und welche nötigen Schritte eingeleitet werden sollten. Eine Prüfung empfiehlt sich auch, wenn man bereits DSGVO-Massnahmen im Unternehmen umgesetzt hat, da gewisse Unterschiede zu berücksichtigen sind.

2. Datenschutz ist Persönlichkeitsschutz

Datenschutz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden. Der Schutz ist weitrechend: Geschützt sind sämtliche Personendaten, d.h. alle Informationen und Angaben, die sich auf eine identifizierte oder identifizierbare Person beziehen resp. einer bestimmten oder bestimmbaren Person zugeordnet werden können. Als Bearbeitung gilt – unabhängig von den angewandten Mitteln und Verfahren (physisch oder elektronisch) – jeder Umgang mit Personendaten (Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen, Vernichten etc.). Das neue Datenschutzgesetz fokussiert sich auf die natürlichen Personen. Daten juristischer Personen sind nicht mehr geschützt.

3. Grundsätze für die Datenbearbeitung

Für die Bearbeitung von Personendaten gelten folgende ineinandergreifende Grundsätze:

Rechtmässigkeit: Daten dürfen nur im Rahmen des rechtlich Zulässigen bearbeitet werden.

Treu und Glaube: Der verfassungsmässige Grundsatz von Treu und Glaube gilt in der gesamten Rechtsordnung und verdeutlicht im Datenschutzrecht, dass eine rechtsmissbräuchliche Datenbearbeitung unzulässig ist.

Verhältnismässigkeit: Es dürfen nur diejenigen und nur so viele Daten bearbeitet werden, wie für den verfolgten Zweck erforderlich sind (Datenvermeidung und Datensparsamkeit). Organisatorisch dürfen nur diejenigen Personen und Stellen Zugriff auf die Daten haben, für deren Aufgabenerfüllung sie notwendig sind.

Zweckbindung: Jede Datenbearbeitung muss einen bestimmten Zweck verfolgen (Datenbeschaffung auf Vorrat ist unzulässig). Die Daten dürfen nur für den festgelegten resp. erkennbaren Zweck bearbeitet werden.

Transparenz: Die Datenbearbeitung muss für die betroffene Person aus den Umständen heraus oder aufgrund einer expliziten Information erkennbar sein.

Privacy by default und by design: Der Grundsatz des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen soll mittels technischer und organisatorischer Massnahmen sicherstellen, dass die Prinzipien der Zweckbindung und Verhältnismässigkeit eingehalten werden.

Richtigkeit: Die bearbeiteten Daten müssen sachlich richtig und in Bezug auf den Zweck der Datenbearbeitung vollständig sein. Falsche Daten müssen berichtigt, gelöscht oder vernichtet werden.

Sicherheit: Die Sicherheit der bearbeiteten Daten muss durch technische und organisatorische Massnahmen gewährleistet sein. Daten müssen insbesondere vor unbeabsichtigter oder widerrechtlicher Veränderung, Löschung oder Vernichtung sowie unbefugtem Zugriff geschützt werden.

Verantwortlich für den Datenschutz ist, wer über Zweck und Mittel der Bearbeitung entscheidet. Datenschutz ist damit Chefsache!

4. Rechtskonforme Bearbeitung von Personendaten

Rechtskonform ist die Bearbeitung von Personendaten dann, wenn sie die allgemeinen Grundsätze der Datenbearbeitung sowie gegebenenfalls zusätzliche rechtliche Erfordernisse einhält. Folgende drei Datenschutzverletzungen sind in der Praxis häufig:

1. Es werden zu viele Daten erhoben.
2. Daten werden nicht oder ungenügend vor unberechtigtem Zugriff oder Verlust geschützt.
3. Falsche und nicht mehr benötigte Daten werden nicht vernichtet.

Neben den Vorschriften des Datenschutzgesetzes können weitere spezialgesetzliche Vorschriften anwendbar sein (z.B. die Geschäftsbücherverordnung).

5. Datenkategorien

Es werden zwei Kategorien von Daten unterschieden.

Personenbezogene Daten:

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Zwischen einer Information auf der einen und einer Person auf der anderen Seite muss also eine Verbindung herstellbar sein, unmittelbar oder mittelbar. Eine unmittelbare Verbindung ist beispielsweise mit dem Namen, der Anschrift oder dem Geburtsdatum gegeben. Eine mittelbare Verbindung erfolgt etwa mittels Zusatzwissen, beispielsweise bei Telefon-, Matrikel- und Sozialversicherungsnummern oder Online-Kennungen wie IP-Adressen und Cookie-Kennungen. Ausreichend ist dabei, wenn die Information die Identifizierung der betroffenen Person theoretisch ermöglicht, es kommt also nicht darauf an, ob die Person tatsächlich identifiziert wird.

Die Informationen müssen sich auf einen lebenden Menschen beziehen. Einzelangaben über juristische Personen, wie Kapitalgesellschaften oder eingetragene Vereine, sind keine personenbezogenen Daten. Etwas anderes gilt nur, wenn sich die Angaben auch auf die hinter der juristischen Person stehenden Personen beziehen, das heisst auf sie «durchschlagen». Dies kann beispielsweise bei der GmbH einer Einzelperson oder bei einer Einzelfirma der Fall sein, wenn enge finanzielle, persönliche oder wirtschaftliche Verflechtungen zwischen der natürlichen und der juristischen Person bestehen.

Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten werden besonders geschützt. Das sind zum Beispiel Gesundheitsdaten, Daten über die ethnische Herkunft sowie religiöse oder weltanschauliche Überzeugungen, Lohndaten.

6. Datenbekanntgabe und -übertragung

Datenbekanntgabe an Dritte

Das Bekanntgeben von Daten ist eine Datenbearbeitung und hat sich daher nach den datenschutzrechtlichen Grundsätzen zu richten. Insbesondere ist eine Datenbekanntgabe

an unberechtigte Dritte oder ausserhalb des Zwecks, zu dem die Daten erhoben wurden, unzulässig, sofern die betroffene Person nicht eingewilligt hat oder entsprechend informiert wurde. Die Bekanntgabe besonders schützenswerter Personendaten oder von Persönlichkeitsprofilen ist widerrechtlich, wenn kein überwiegendes Interesse oder keine gesetzliche Grundlage besteht. (Zudem gilt hier bei der Beschaffung eine Informationspflicht.)

Auftragsbearbeitung

Werden die Daten im Auftrag des Verantwortlichen durch einen Dritten bearbeitet, muss dieser Auftragsbearbeiter die gleichen Bestimmungen einhalten wie der Verantwortliche. Zudem darf der Auftragsbearbeitung keine gesetzliche oder vertragliche Geheim-haltungspflicht entgegenstehen.

Datenbekanntgabe ins Ausland

Personendaten dürfen nur dann ins Ausland bekannt gegeben werden, wenn die Gesetzgebung des betreffenden Staates ein angemessenes Schutzniveau gewährleistet. (Der EDÖB führt eine entsprechende Staatenliste.) Ausnahmsweise ist eine Datenbekanntgabe in ein Land ohne angemessenes Schutzniveau möglich, wenn zusätzliche Schutzmassnahmen getroffen werden.

Auskunftspflicht

Jede Person kann beim Verantwortlichen Auskunft darüber verlangen, ob über sie Personendaten bearbeitet werden. Das Auskunftsrecht erstreckt sich auf alle Informationen, die erforderlich sind, damit die betroffene Person ihre Datenschutzrechte geltend machen kann. Der Verantwortliche kann die Auskunft ausnahmsweise verweigern oder einschränken.

Pflicht zur Berichtigung

Der Verantwortliche muss auf Verlangen der betroffenen Person unrichtige Daten berichtigen.

Herausgabe- und Übertragungspflicht

Das neue Datenschutzgesetz hält explizit fest, dass jede Person die Herausgabe resp. Übertragung ihrer Personendaten, die sie dem Verantwortlichen bekanntgegeben hat, in einem gängigen elektronischen Format verlangen kann.

Datenschutzberater

Freiwillig ist die Ernennung eines Datenschutzberaters, der als Anlaufstelle für die betroffenen Personen oder für die Behörden dient.

7. Datensicherheit

Bei der Datensicherheit handelt es sich um technische Massnahmen, die getroffen werden sollten, um Daten vor Verlust, Manipulation, Fremdzugriff, Viren usw. zu schützen.

Welche technischen und personellen Massnahmen zum Schutz vor Datenverlust und dem unberechtigten Zugriff getroffen werden müssen, ist abhängig von der individuellen IT-Infrastruktur und somit Sache des Unternehmens. Details hierzu sind im Leitfaden für IT-Security (Datenschutz) unter folgendem Link zu finden: https://bit.ly/30UayX3

In der Regel unterstützen getroffene Massnahmen in der Datensicherheit den Datenschutz. Aber es kann auch zu neuen Konflikten und Fragen führen. So kann die Auslagerung des Backups in die Cloud oder auf ein Fremdsystem Risiken beim Datenschutz schaffen, da dadurch Daten von Unberechtigten eingesehen oder heruntergeladen werden können. Dem ist durch entsprechende Massnahmen entgegen zu wirken und vorab genau zu prüfen.

8. Aufbewahrung, Rückgabe und Vernichtung von Daten

Personenbezogene Daten dürfen von Unternehmen nur für eindeutige und legitime Zwecke erhoben und verarbeitet werden – dies besagt die sogenannte Zweckgebundenheit. Das heisst konkret, dass die erhobenen Daten gelöscht oder allenfalls anonymisiert werden müssen, sobald der Zweck, für den Sie erhoben wurden – zum Beispiel eine Reklamation – erfüllt wurde. Liegt eine gesetzliche Aufbewahrungsfrist für die personenbezogenen Daten vor, müssen diese erst nach Ablauf der Aufbewahrungsfrist gelöscht werden. In der Praxis haben sich bis heute zwei praktikable Wege verbreitet. Die Unkenntlichmachung (Maskierung von Daten), sowie die Verschlüsselung / Zugriffsberechtigungs-Einschränkung mit einer Einwilligungserklärung der jeweiligen Betroffenen Personen. Meistens Bestandteil von AGB's oder Personalreglemente etc.

9. Neue Governance-, Informations- und Sorgfaltspflichten

Das neue Datenschutzgesetz, das voraussichtlich 2023 in Kraft treten wird, sieht gegenüber dem geltenden Recht bei der Datenbearbeitung zusätzliche Governance- und Informationspflichte vor, deren vorsätzliche Verletzung zu Bussen bis 250'000 Franken führen kann.

Verzeichnis der Bearbeitungstätigkeiten

Verantwortliche und Auftragsbearbeiter müssen nach neuem Datenschutzgesetz ein Verzeichnis ihrer Bearbeitungstätigkeiten führen, das mindestens folgende Angaben enthalten muss: Identität des Verantwortlichen, Bearbeitungszweck, Beschreibung der betroffenen Kategorien Personen und Personendaten, die Kategorien der Datenempfänger, Aufbewahrungsdauer und Kriterien zur Festsetzung der Dauer, Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit, bei Bekanntgabe ins Ausland die Angabe des Staates und allfälliger Schutzgarantien.

Informationspflicht

Wer Personendaten beschafft, informiert die betroffene Person angemessen über die Beschaffung. Die Information umfasst mindestens die Identität und die Kontaktdaten des Verantwortlichen, den Bearbeitungszweck und gegebenenfalls Dritten oder die Kategorie von Dritten, denen Personendaten bekanntgegeben werden. Die Informationspflicht entfällt, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt, die Bearbeitung gesetzlich vorgeschrieben ist oder wenn der Verantwortliche gesetzlich zur Geheimhaltung verpflichtet ist.

Datenschutz-Folgeabschätzung

Sofern die Bearbeitung von Personendaten ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, muss der Verantwortliche vorgängig seine Datenschutz-Folgeabschätzung mit einer Beschreibung der geplanten Bearbeitung, einer Risikobewertung und Massnahmen erstellen.

Meldepflicht

Verletzungen der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führen, müssen so rasch wie möglich dem EDÖB und allenfalls den betroffenen Personen gemeldet werden.

10. Rechtsfolgen bei Datenschutzverletzungen oder administrativer Pflichten

Unter dem geltenden Datenschutzgesetz können Personen, die durch eine unzulässige Datenbearbeitung in ihrer Persönlichkeit verletzt sind, zivilrechtlich Klage zum Schutz ihrer Persönlichkeit erheben und insbesondere verlange, dass die Datenbearbeitung gesperrt wird, keine Daten an Dritte bekannt gegeben werden oder Personendaten berichtigt oder vernichtet werden.

Das neue Datenschutzgesetz sieht zusätzlich zu den zivilrechtlichen Ansprüchen bei der Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten sowie von Sorgfaltspflichten eine strafrechtliche Haftung vor: Bei vorsätzlicher Verletzung der Pflichten drohen Bussen bis 250'000 Franken.

11. Best Practice im Treuhandunternehmen: Praxistipps

- Mit einfachen Massnahmen sich gegen das Risiko einer Datenschutzverletzung absichern
    - Saubere Auslegeordnung der IT-Infrastruktur (intern und extern) erstellen, um mögliche Problempunkte zu erkennen. Diese Punkte in einem zweiten Schritt beheben.
    - Das Thema mit den Kunden ansprechen z.B. im Zug einer Abschlussbesprechung. Direkt Lösungsvorschläge machen (z.B. beim unverschlüsselten Versand von personenbezogenen Daten)
    - Bereiche auflisten, wo potentielle Fallen bestehen (z.B. Lohnbuchhaltung, Ablage Buchungsunterlagen mit personenbezogenen Daten). Für diese Fallen Handhabungen definieren
    - Den Mitarbeitenden die Gefahren aufzeigen, die im Umgang mit E-Mails und mobilen Endgeräten auftreten können. Hierzu Lösungen und Handlungsregeln definieren
    - Auftragsbestätigungen mit entsprechenden Passagen zum Datenschutz und Datenhaltung erstellen
- Beispiele von Grobfahrlässigkeit beim Umgang mit Daten bei einem Treuhänder
    - Lohndaten unverschlüsselt an Kunde oder direkt an Mitarbeiter senden ohne deren explizite Zustimmung
    - Zugriffe auf Daten nicht anhand Zuständigkeit/Verantwortlichkeit geregelt
    - Verwenden von Cloud-Lösungen ohne die Anwendung einer 2-Faktoren Authentifizierung (Grundsätze zur Cloud-Sicherheit missachtet)
    - Dem Schutz von personenbezogenen Daten (intern oder extern gespeichert) werden keine besondere Aufmerksamkeit geschenkt

12. Weiterführende Informationen

- Webseite des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB): www.edoeb.admin.ch
- Grundbekenntnis der Schweizer Wirtschaft zu einem verantwortungsvollen Umgang mit Daten: www.economiesuisse.ch/de/datenwirtschaft
- EDÖB-Liste der Staaten, deren Gesetzgebung einen angemessenen Datenschutz gewährleisten: https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2020/staatenliste.pdf.download.pdf/20200908_Staatenliste_d.pdf
- Leitfaden vom Institut Treuhand 4.0 für IT-Security (Datenschutz): https://bit.ly/30UayX3