Richtlinie der HIAG-Gruppe zum Datenschutz

1. Mai 2024

1. Zweck

Die HIAG Immobilien Holding AG, Basel, Schweiz (das "**Unternehmen**") hat diese Richtlinie zur Regelung des Umgangs mit Personendaten von Kunden und Mitarbeitenden des Unternehmens erlassen. Der Begriff "Unternehmen" umfasst alle Tochtergesellschaften des Unternehmens in der Schweiz. Der Verlust von Personendaten kann zu erheblichen Schäden für Einzelpersonen führen, einschliesslich Offenlegung heikler Daten, Unannehmlichkeiten und betrügerischer Nutzung der Informationen. Der Schutz der Vertraulichkeit und Integrität von Personendaten ist eine wichtige Aufgabe, die jederzeit ernst genommen werden muss. Die Einhaltung dieser Datenschutzrichtlinie ("Richtlinie") ist Pflicht. Bitte beachten Sie, dass die Rechte von Personen je nach geltender Rechtsordnung variieren können.

Der Zweck dieser Richtlinie ist:

- Die Definition von Personendaten und besonders schützenswerten Personendaten.
- Die Festlegung allgemeiner Grundsätze für den Schutz von Personendaten.
- Die Regelung der Zuständigkeit für den Schutz von Personendaten.
- Strafrechtlichen Risiken vorzubeugen (namentlich falsche oder unvollständige Auskünfte können Bussen bis CHF 250'000 nach sich ziehen).
- Abläufe und Vorlagen bei Auskunftsgesuchen und Datensicherheitsverletzungen sowie Datenschutz-Folgenabschätzungen bereitzustellen (siehe namentlich die **Anhänge 1 bis 3**).

2. Umfang

Diese Richtlinie gilt für alle Mitarbeitenden des Unternehmens ("**Sie**") sowie Agenten und Vertreter, die Zugriff auf Personendaten haben, die das Unternehmen erhoben hat oder anderweitig in seinem Besitz hat. Diese Richtlinie gilt für alle Personendaten, die vom Unternehmen erhoben, verwaltet, übertragen, gespeichert, aufbewahrt, verändert, bekanntgegeben, gelöscht, vernichtet oder anderweitig verwendet werden, unabhängig davon, ob sie sich auf Mitarbeitende, Kunden oder andere natürliche Personen beziehen.

3. Definitionen

"Auftragsbearbeiter" wird untenstehend bei **"Verantwortlicher"** definiert und abgegrenzt.

"Bearbeitung" bezeichnet jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren. Der Begriff der Bearbeitung ist sehr weit zu verstehen und

bezieht sich nicht nur auf die digitale Bearbeitung und Auswertung von elektronischen Daten, sondern auch von physischen Unterlagen, z.B. Papierakten. Bearbeitungstypen sind insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, aktive Übermitteln, passive Zugänglichmachen, Archivieren, Löschen oder Vernichten von Personendaten.

"Betroffener" bezeichnet eine bestimmte oder bestimmbare natürliche Person, deren Personendaten bearbeitet werden.

"DSG" bezeichnet das schweizerische Bundesgesetz über den Datenschutz vom 25. September 2020.

"DSGVO" bezeichnet die Datenschutz-Grundverordnung der Europäischen Union (Verordnung (EU) 2016/679).

"DSV" bezeichnet die schweizerische Verordnung über den Datenschutz vom 31. August 2022.

"Personendaten" sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Eine bestimmbare natürliche Person ist eine Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Bezugnahme auf einen Identifikator wie einen Namen, eine Identifikationsnummer, Standortdaten, einen Online-Kennzeichner oder auf einen oder mehrere Faktoren, die spezifisch für die physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität dieser natürlichen Person sind. Zu diesen Informationen gehören unter anderem:

- Namen;
- Adressen;
- Telefonnummern;
- E-Mail-Adressen;
- Mitarbeiteridentifikationsnummern;
- AHV-Nummer;
- Benutzeridentifikation und Zugangsdaten für das Konto, Passwörter, PINs und Antworten auf Sicherheitsfragen;
- Bankkontonummern;
- Bild- und Tonaufnahmen;
- technische Daten (z.B. IP-Adresse);
- Geolokalisierungsdaten; und

- biometrische, medizinische, gesundheitliche oder krankenversicherungstechnische Informationen.

"Besonders schützenswerte Personendaten" sind Personendaten, für deren Bearbeitung gegenüber der Bearbeitung von einfachen Personendaten (z.B. Adresse, Lohn) zum Teil strengere rechtliche Anforderungen gelten. Diese Qualifikation rührt daher, dass die als besonders schützenswert bezeichneten Datenkategorien nach Auffassung des Gesetzgebers die Persönlichkeit der Betroffenen derart stark berühren, dass ihre Bearbeitung immer eine Beeinträchtigung der Persönlichkeit darstellt. Beispiele für besonders schützenswerte Personendaten sind:

- biometrische, medizinische, gesundheitliche (physischer und psychischer Gesundheitszustand) oder krankenversicherungstechnische Informationen;
- religiöse und weltanschauliche Überzeugungen sowie politische Meinungen;
- Gewerkschaftsmitgliedschaft;
- Sozialversicherungsleistungen im Zusammenhang mit Krankheit und Unfall;
- Zugehörigkeit zu einer Rasse oder Ethnie; und
- Strafregistereinträge.

In den meisten Rechtsordnungen definiert das Gesetz die Arten von Informationen, die einem erhöhten Schutz unterliegen. Wenn Sie Fragen dazu haben, ob Personendaten als besonders schützenswerte Personendaten eingestuft werden können, wenden Sie sich bitte an den General Counsel.

"Datensicherheitsverletzung" bezeichnet jede Handlung oder Unterlassung durch eine interne oder externe Person, welche die Sicherheit, Vertraulichkeit oder Integrität von Personendaten oder die physischen, technischen, administrativen oder organisatorischen Sicherheitsvorkehrungen, die das Unternehmen oder ein Drittdienstleister zum Schutz von Personendaten getroffen hat, beeinträchtigt. Der Verlust, die unbeabsichtigte oder widerrechtliche Löschung, Vernichtung, Veränderung oder der unbefugte Zugriff auf Personendaten sowie ihre Offenlegung vor Unbefugten sind Datensicherheitsverletzungen.

"Verantwortlicher" ist die natürliche oder juristische Person, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Bearbeitung bestimmt. Dies als Abgrenzung zum **"Auftragsbearbeiter"**, der bloss im Auftrag des Verantwortlichen Personendaten bearbeitet. Zur Unterscheidung der beiden Rollen:

Eine Auftragsbearbeitung liegt gemäss DSG (und auch im Sinne der DSGVO) dann vor, wenn

(a) ein Auftragnehmer (d.h. der Auftragsbearbeiter) im Auftrag eines Auftraggebers (d.h. des Verantwortlichen) Personendaten bearbeitet,

(b) der Auftragnehmer die Daten nur für die Zwecke der Auftragserfüllung bearbeiten darf (und nicht für eigene Zwecke),

(c) der Auftragnehmer die Daten nach den Weisungen/Vorgaben des Auftraggebers bearbeitet – ohne, dass der Auftragnehmer über grosse eigene Autonomie bei der Erfüllung des Auftrages verfügt, und

(d) der Schwerpunkt der Dienstleistung in einer Datenbearbeitung liegt (z.B. beim Datenhosting in der Form des Speicherns von Daten). Wenn der Schwerpunkt der Dienstleistung dagegen nicht in einer Datenbearbeitung liegt, muss keine Auftragsbearbeitungsvereinbarung abgeschlossen werden bzw. liegt keine Auftragsbearbeitung vor.

4. Bearbeitungvon Personendaten

4.1 Faire und rechtmässige Bearbeitung

4.1.1 Im Allgemeinen

Wann immer das Unternehmen Personendaten bearbeitet, muss das Unternehmen sicherstellen, dass die Bearbeitung rechtmässig, fair und transparent gegenüber dem Betroffenen erfolgt.

Für bestimmte Bearbeitungsvorgänge fungiert das Unternehmen als Verantwortlicher, gemeinsamer Verantwortlicher oder für andere als Auftragsbearbeiter. Wenn das Unternehmen als Verantwortlicher tätig ist, muss das Unternehmen sicherstellen, dass es seinen datenschutzrechtlichen Pflichten nachkommt: die meisten Pflichten des DSG (und auch der DSGVO) treffen den Verantwortlichen. Zentral ist bspw. die Informationspflicht: Betroffene sind transparent über Personendatenbearbeitungen zu informieren. Daneben muss der Verantwortliche Auftragsbearbeitungsvereinbarungen (engl. Data Processing Agreements, oft mit **"DPA"** abgekürzt) mit von ihm eingesetzten Auftragsbearbeitern abschliessen.

Wenn das Unternehmen als Auftragsbearbeiter tätig ist, bearbeitet das Unternehmen im Allgemeinen Personendaten im Auftrag seiner Kunden. In diesen Fällen ist der Kunde dafür zuständig, die grundlegenden Pflichten des DSG (oder je nachdem der DSGVO) einzuhalten. Das Unternehmen hat jedoch auch in diesen Fällen sorgfältig mit den Personendaten umzugehen. Insbesondere sämtliche Pflichten des abgeschlossenen DPA mit dem Kunden sind einzuhalten, um Schadenersatzansprüchen vorzubeugen.

4.1.2 Ausnahmsweise Anwendbarkeit der DSGVO

Das Unternehmen untersteht bei seinen Datenbearbeitungen grundsätzlich dem schweizerischen Datenschutzrecht und hat sich somit am DSG und der DSV zu orientieren. In der EU und dem EWR (Norwegen, Island und Fürstentum Liechtenstein) gilt hingegen die

DSGVO. Das DSG und die DSV sind grundsätzlich liberaler als die DSGVO – namentlich hinsichtlich der einzuhaltenden Pflichten und auch bezüglich der Strafandrohungen bei Pflichtverletzungen.

Die DSGVO muss von Schweizer Gesellschaften jedoch in gewissen Fällen beachtet werden:

Wenn eine Schweizer Gesellschaft eine Niederlassung (d.h. Tochtergesellschaft, Filiale, Zweigniederlassung) in der EU/dem EWR hat, muss (nur) diese Niederlassung die DSGVO beachten.

Wenn Dienstleistungen und Waren an Personen in der EU/dem EWR angeboten werden, muss die DSGVO (nur) hinsichtlich dieser ausländischen Kunden/Endkunden beachtet werden.

Wenn Tracking-Tools (z.B. Google Analytics) eingesetzt werden und dabei das Verhalten von Personen mit Aufenthalt in der EU/dem EWR beobachtet werden. Auch hier gilt die DSGVO nur hinsichtlich dieser ausländischen Personen.

Und schliesslich auch, wenn eine Schweizer Gesellschaft als Auftragsbearbeiter für eine Gesellschaft Daten bearbeitet, die ihrerseits der DSGVO untersteht. Dann wird regelmässig auch das DPA nach DSGVO abgeschlossen.

Eine zentrale Unterscheidung zwischen DSG und DSGVO ist die der Rechtfertigung bzw. der notwendigen Rechtgrundlagen:

Für die *Verarbeitung personenbezogener Daten* nach DSGVO ist eine Rechtsgrundlage erforderlich, für die *Bearbeitung von Personendaten* nach DSG in der Regel nicht. Das DSG setzt im Gegensatz zur DSGVO keine Rechtfertigung für Datenbearbeitungen voraus – Personendaten dürfen bearbeitet werden, solange die Bearbeitungsgrundsätze (siehe nachfolgend ab Ziff. 4.2, z.B. Richtigkeit und Zweckbindung) eingehalten sind. Rechtfertigungsgründe sind nach DSG nur im Zusammenhang mit Persönlichkeitsverletzungen relevant. Personenbezogene Daten dürfen gemäss DSGVO jedoch nur dann verarbeitet werden, wenn mindestens eine der folgenden Rechtsgrundlagen vorliegt, wobei namentlich die Einwilligung in gewissen Fällen auch nach DSG eine Rolle spielt, wenn besonders schützenswerte Personendaten bearbeitet werden:

Einwilligung: *Die Einwilligung ist die einfachste Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Wichtig zu beachten ist, dass die Einwilligung freiwillig, spezifisch, informiert und unmissverständlich erteilt werden muss. Die Einwilligung kann durch schriftliche oder mündliche Erklärung oder auch auf elektronischem Wege erfolgen, wie z.B. durch Ankreuzen eines Kästchens beim Besuch einer Website, sofern damit die Einwilligung zur Verarbeitung deutlich erkennbar ist. Schweigen, vorgemerkte Kästchen oder Inaktivität gelten nicht als Einwilligung.*

*Wann immer Unternehmen **sensible** personenbezogene Daten – oder gemäss DSG **besonders schützenswerte** Personendaten – verarbeiten, ist eine **ausdrückliche** Einwilligung der betroffenen Person erforderlich. Gemäss DSGVO immer, gemäss DSG nur dann, wenn das DSG eine solche ausnahmsweise Einwilligung überhaupt als Voraussetzung vorsieht – das ist vor allem bei Auslandsdatenbekanntgaben und automatisierten Einzelentscheidungen der Fall, aber z.B. auch, wenn Dritten Gesundheitsdaten bekanntgegeben werden.*

Eine Einwilligung kann jederzeit widerrufen werden, und der Widerruf der Einwilligung sollte so einfach wie die Erteilung der Einwilligung möglich sein. Der Widerruf berührt die Rechtmässigkeit der davor geschehenen Verarbeitung nicht.

***Vertragliche Notwendigkeit:** Die Verarbeitung personenbezogener Daten ist gerechtfertigt, wenn die Verarbeitung für die Erfüllung eines Vertrags erforderlich ist, an dem die betroffene Person beteiligt ist.*

***Einhaltung rechtlicher Verpflichtungen:** Das Unternehmen ist berechtigt, personenbezogene Daten zu verarbeiten, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.*

***Lebensnotwendige Interessen:** Die Verarbeitung ist zulässig, wenn sie zum Schutz der wesentlichen Interessen der betroffenen Person oder einer anderen Person erforderlich ist.*

***Öffentliches Interesse:** Das öffentliche Interesse umfasst die Verarbeitung, die für ein bestimmtes öffentliches Interesse erforderlich ist. Beispiele sind Steuern, Anzeige eines Vergehens oder Verbrechens, öffentliche Gesundheit sowie Qualität und Sicherheit von Produkten.*

***Berechtigtes Interesse:** Ein berechtigtes Interesse kann als Vorteil für ein Unternehmen oder eine Gesellschaft als Ganzes bezeichnet werden, der sich aus der Verarbeitung personenbezogener Daten ergeben kann. Wann immer das Unternehmen ein berechtigtes Interesse als Grundlage für die Verarbeitung verwenden möchte, muss das Unternehmen sicherstellen, dass ein Ausgleich zwischen dem Interesse des Unternehmens und den Rechten und Interessen der betroffenen Person hergestellt wird.*

4.2 Benachrichtigung und Beschaffung von Daten sowie Zweckbindungsgrundsatz

Es gehört zu den Grundsätzen des Unternehmens, dass es, wenn es Personendaten für einen bestimmten Zweck, einschliesslich für Personal- oder Beschäftigungszwecke, beschafft, die Betroffenen darüber informieren muss, wie es diese Personendaten verwenden, speichern, offenlegen, schützen und aufbewahren wird, indem es dem Betroffenen zum Zeitpunkt der Beschaffung der Personendaten eine Datenschutzerklärung oder einen

Datenschutzhinweis vorlegt (Transparenzgrundsatz; siehe auch Ziff. 4.7). Sie dürfen Personendaten nur in Übereinstimmung mit den geltenden Unternehmensrichtlinien, Mitteilungen und – sofern die DSGVO anwendbar ist – der Einwilligung des Betroffenen beschaffen, und die beschafften Personendaten müssen auf das beschränkt sein, was vernünftigerweise notwendig ist, um die legitimen Geschäftszwecke des Unternehmens zu erfüllen, oder wenn dies zur Einhaltung des Gesetzes erforderlich ist. Der Grundsatz der Zweckbindung lässt sich somit wie folgt zusammenfassen: Personendaten dürfen nur zu dem Zweck, der bei der Beschaffung der Daten dem Betroffenen mitgeteilt worden ist oder der für ihn ersichtlich war (legitime Geschäftszwecke des Unternehmens), bearbeitet werden.

4.3 Zugang, Nutzung und Weitergabe von Personendaten

Sie dürfen nur dann auf Personendaten zugreifen, wenn sich diese Informationen auf Ihre beruflichen Aufgaben beziehen und zur Erfüllung Ihrer beruflichen Aufgaben erforderlich sind. Sie dürfen aus keinem Grund, der nicht mit Ihren beruflichen Aufgaben zusammenhängt, auf Personendaten zugreifen. Sie dürfen Personendaten nicht in einer Weise verwenden, die mit der Mitteilung an den Betroffenen zum Zeitpunkt der Datenerfassung unvereinbar ist. Wenn Sie sich nicht sicher sind, ob eine bestimmte Verwendung oder Offenlegung angemessen ist, sollten Sie sich an den General Counsel wenden. Sie dürfen Personendaten nur dann an einen anderen Mitarbeitenden des Unternehmens weitergeben, wenn der Empfänger ein berufsbedingtes Bedürfnis hat, die Informationen zu kennen. Personendaten dürfen nur dann an einen Drittdienstleister, Agenten oder Vertreter weitergegeben werden, wenn dieser die Informationen für die Erbringung der vertraglich vereinbarten Dienstleistungen kennen muss und wenn die Weitergabe der Personendaten mit den Datenschutzhinweisen für die betroffene Person übereinstimmt. Diesfalls ist auch zu prüfen, ob ein DPA mit dem Drittdienstleister, Agenten oder Vertreter abgeschlossen wurde. Sollte dies nicht der Fall sein, ist dieser Umstand dem General Counsel zu melden.

4.4 Richtigkeit

Sie dürfen nur Personendaten erheben, pflegen und verwenden, die korrekt, vollständig und relevant für die Zwecke sind, für die sie erhoben wurden. Fehlerhafte Daten sind zeitnah zu löschen oder zu korrigieren.

4.5 Datensicherheit

Sie sind für den Schutz von Personendaten im Unternehmen zuständig. Das Unternehmen hat eine Informationssicherheitsrichtlinie implementiert, die technische, administrative und physische Sicherheitsvorkehrungen für den Schutz von Personendaten festlegt. Sie müssen die in der Informationssicherheitsrichtlinie festgelegten Sicherheitsverfahren jederzeit einhalten. Sie müssen besondere Sorgfalt walten lassen, um besonders schützenswerte Personendaten vor Verlust, unbefugtem Zugriff und unbefugter Weitergabe zu schützen.

4.6 Verhältnismässigkeitsprinzip sowie Datenminimierung und Löschung

Personendatenbearbeitungen müssen geeignet und objektiv erforderlich sein, um ein legitimes Ziel zu erreichen. Das führt dazu, dass nur so viele Personendaten erhoben und bearbeitet werden dürfen, wie es der Zweck erfordert. Sobald die Personendaten nicht mehr benötigt werden, sind sie zu löschen oder zu anonymisieren.

4.7 Transparenz und Gruppen-Datenschutzerklärung

Bei der Bearbeitung von Personendaten muss das Unternehmen transparent sein. Die Transparenz bezieht sich auf das Recht des Betroffenen, die Kontrolle über seine Personendaten zu behalten, und verpflichtet das Unternehmen, die nötigen Massnahmen zu ergreifen, um sicherzustellen, dass die erforderlichen Informationen an den Betroffenen weitergegeben werden. Dem Betroffenen müssen bei der Beschaffung seiner Personendaten die nachfolgenden Informationen mitgeteilt werden:

- die Identität und die Kontaktdaten des Verantwortlichen;
- die Bearbeitungszwecke;
- gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden.

Im Einzelfall können zudem weitere Informationen verlangt sein, wenn die nachfolgenden Voraussetzungen gegeben sind:

- Falls die Personendaten nicht beim Betroffenen beschafft werden, müssen ihm die Kategorien der bearbeiteten Personendaten mitgeteilt werden.
- Falls die Personendaten ins Ausland bekanntgegeben werden, müssen dem Betroffenen auch der jeweilige Staat und gegebenenfalls die getroffenen Schutzvorkehrungen mitgeteilt werden.

Letztendlich bedeutet transparentes Handeln, dass das Unternehmen dem Betroffenen alle Informationen im Zusammenhang mit der Bearbeitung mitteilen sollte und dass das Unternehmen diese Informationen in klarer und verständlicher Sprache leicht zugänglich und leicht verständlich macht. Das Unternehmen muss die betroffene Person auf die Risiken, Regeln, Garantien und Rechte im Zusammenhang mit der Bearbeitung aufmerksam machen. Das Unternehmen hat auf seiner Webseite eine Gruppen-Datenschutzerklärung veröffentlich: https://www.hiag.com/de/datenschutzerklaerung/. Betroffene müssen nicht explizit auf diese Datenschutzerklärung hingewiesen werden; dies kann aber im Einzelfall sinnvoll sein (vor allem wenn besonders schützenswerte Personendaten bearbeitet werden, zu Beginn einer neuen Vertragsbeziehung oder bei Einführung neuer technischer Applikationen [z.B. einer Mobile-App]). Die Datenschutzerklärung ist eine einseitige Information des Unternehmens, kann jederzeit angepasst werden und wird nicht Bestandteil von Verträgen

mit Betroffenen. Deswegen müssen die Betroffenen auch keine Einwilligung zur Gruppen-Datenschutzerklärung abgeben.

4.8 Rechte der Betroffenen

Personen haben Rechte, wenn es um den Umgang mit ihren Personendaten geht. Diese Rechte können je nach geltender Rechtsordnung variieren, können aber beispielsweise Folgendes umfassen:

4.8.1 Auskunftsrecht – Handhabung von Auskunftsgesuchen

Jede Person kann vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Solche Auskunftsbegehren werden in der Regel schriftlich gestellt (durch den Betroffenen oder seinen Anwalt) und sind in den meisten Fällen kostenlos, schriftlich sowie innert 30 Tagen zu beantworten. Sollte ein Auskunftsgesuch mündlich gestellt werden, muss der Betroffene gebeten werden, sein Gesuch auf schriftlichem Wege zu wiederholen. Zudem muss immer eine Ausweiskopie der antragstellenden Person verlangt werden (bzw. eine Anwaltsvollmacht).

Bei der Beantwortung sind vor allem drei Dinge wichtig und in jedem Fall zu beachten: (i) Bei einer Auskunftserteilung darf niemals eine Vollständigkeitserklärung abgegeben werden, (ii) wenn sich das Auskunftsbegehren explizit oder implizit auf konkrete Auskünfte bezieht, sind nur diese und keine weiteren Auskünfte zu erteilen und (iii) falls das Auskunftsgesuch datenschutzfremden oder sogar datenschutzwidrigen Zwecken dienen könnte, ist das Auskunftsgesuch nicht zu beantworten und stattdessen auf diesen Umstand aufmerksam zu machen. Das Auskunftsrecht darf nämlich unter keinen Umständen der Beweismittelbeschaffung (z.B. bei einem möglichen Rechtsstreit) oder der Buchführung eines Betroffenen dienen. Auch offensichtlich querulatorische Gesuche oder wiederholt gestellte Gesuche sind abzuweisen.

Näheres zum zwingend einzuhaltenden Ablauf und eine Vorlage für einen Antwortbrief auf Auskunftsgesuche finden sich in **Anhang 3**.

4.8.2 Recht auf Löschung

In der Schweiz gibt es, anders als in der EU und dem EWR, kein Recht auf Vergessenwerden. Ein Betroffener kann jedoch vom Verantwortlichen verlangen, seine Personendaten zu löschen und nicht mehr zu bearbeiten. Diese Anfrage kann gestellt werden, weil (i) die Bearbeitung im Hinblick auf den Zweck, für den die Personendaten erhoben werden, nicht mehr erforderlich ist oder (ii) die betroffene Person von ihrem Recht auf Widerruf Gebrauch gemacht hat oder (iii) die Personendaten unrechtmässig bearbeitet werden oder (iv) die Löschung gesetzlich vorgeschrieben ist.

4.8.3 Widerspruchsrecht

Der Betroffene hat das Recht, dem Direktmarketing jederzeit zu widersprechen (z.B. Abbestellen des Newsletters). In diesem Fall ist das Unternehmen verpflichtet, die Verwendung der Personendaten für Marketingzwecke einzustellen.

4.8.4 Recht auf Datenherausgabe oder -übertragung

Der Betroffene kann einerseits verlangen, dass der Verantwortliche ihm die Personendaten herausgibt, die er ihm bekanntgegeben hat und andererseits, dass der Verantwortliche die Personendaten des Betroffenen an einen anderen Verantwortlichen überträgt. Dabei muss das Unternehmen sicherstellen, dass dies in einem gängigen elektronischen Format geschieht, was nur bei elektronisch bearbeiteten Daten möglich ist – deswegen besteht kein Anspruch auf Herausgabe oder Übertragung von Personendaten, wenn ausschliesslich Papierakten vorliegen (im Einzelfall darf der Anfrage auf Herausgabe jedoch nachgekommen werden, wenn kein unverhältnismässiger Aufwand mit dem Nachkommen der Anfrage verbunden ist).

4.8.5 Strafrechtliche Sanktionen

Sie müssen die geltenden Gesetze in Bezug auf die Rechte der Betroffenen einhalten. Wenn Sie sich nicht sicher sind, welche gesetzlichen Anforderungen gelten, oder wenn Sie eine Anfrage oder Beschwerde von einer betroffenen Person bezüglich der Bearbeitung ihrer Personendaten erhalten, wenden Sie sich bitte umgehend an die Rechtsabteilung. Dies ist vor allem deswegen wichtig, weil z.B. Auskunftsgesuche innert 30 Tagen beantwortet werden müssen und bei falscher Auskunft strafrechtliche Sanktionen drohen können. In der Schweiz drohen Bussen bis CHF 250'000.00, wenn Informations-, Auskunfts-, Mitwirkungs- und Sorgfaltspflichten verletzt werden. In der EU und im EWR sind die Strafbestimmungen strenger und es sind höhere Bussen möglich.

5. Datenschutz-Folgenabschätzung

Vor der Einführung eines neuen Systems oder Geschäftsprozesses, wodurch Personendaten bearbeitet werden, sollte eine Datenschutz-Folgenabschätzung durchgeführt werden (siehe auch **Anhang 2**), wenn die Personendatenbearbeitung ein hohes Risiko für die Persönlichkeit des Betroffenen mit sich bringen kann. Das hohe Risiko ergibt sich bspw. bei Verwendung neuer Technologien oder der umfangreichen Bearbeitung besonders schützenswerter Personendaten.

Der Zweck der Datenschutz-Folgenabschätzung besteht darin, solche hohen Risiken zu erkennen und zu bewerten, die eine neue Datenbearbeitung für die Persönlichkeit des Betroffenen mit sich bringen kann. Bei der Erstellung der Datenschutz-Folgenabschätzung

können Massnahmen identifiziert und definiert werden, welche diese Risiken vermeiden oder verringern Nähere Informationen und ein Fragebogen finden sich in **Anhang 2**.

6. Aufbewahrung und Löschung

In der Regel müssen alle gespeicherten Personendaten, die nicht mehr zur Erreichung des Zwecks der Bearbeitung erforderlich sind, dauerhaft gelöscht werden, es sei denn, für die fraglichen Personendaten gilt eine gesetzliche Aufbewahrungsfrist oder es gibt einen anderen legitimen Grund zu deren Speicherung. Um dieser Anforderung gerecht zu werden, hat das Unternehmen (i) maximale Aufbewahrungsfristen für alle gespeicherten Personendaten und (ii) regelmässige Überprüfungsprozesse zusammen mit Mechanismen zur Bereinigung von Personendaten eingeführt.

Das Unternehmen wird Daten auf seinen Systemen über den längsten der folgenden Zeiträume aufbewahren: (i) solange dies für die betreffende Tätigkeit oder die betreffenden Dienstleistungen notwendig oder nützlich ist; (ii) jede gesetzlich vorgeschriebene Aufbewahrungsfrist; oder (iii) das Ende des Zeitraums, in dem Rechtsstreitigkeiten oder Untersuchungen in Bezug auf Dienstleistungen entstehen könnten (in der Schweiz sind das oft 10 Jahre). Sie müssen die geltenden Zeitpläne und Richtlinien zur Aufbewahrung von Aufzeichnungen befolgen und alle Datenträger, die Personendaten enthalten, in Übereinstimmung mit den geltenden Richtlinien zur Entsorgung von Aufzeichnungen, falls vorhanden, vernichten.

7. Bekanntgabe von Personendaten ins Ausland

In einigen Fällen kann das Unternehmen Personendaten an Empfänger weitergeben, die ihren Sitz in Ländern ausserhalb der Europäischen Union (EU), dem Europäischen Wirtschaftsraum (EWR) und der Schweiz haben, deren Gesetze oftmals nicht das gleiche Schutzniveau für Personendaten bieten. In solchen Fällen muss das Unternehmen sicherstellen, dass es angemessene Sicherheitsvorkehrungen trifft, die den gesetzlichen Verpflichtungen des Unternehmens entsprechen. Oft werden in solchen Fällen Standarddatenschutzklauseln verwendet, die der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) genehmigt bzw. anerkannt hat (wichtig sind hier die Standardvertragsklauseln der Europäischen Kommission). Daneben ist es auch denkbar, dass der Betroffene ausdrücklich und schriftlich in die Auslandsbekanntgabe eingewilligt hat (solche Einwilligungen müssen in jedem Fall aufbewahrt werden). Weil auch bei Auslandsdatenbekanntgaben strafrechtliche Sanktionen drohen können, ist vor heiklen Bekanntgaben (z.B., wenn besonders schützenswerte Personendaten betroffen sind) in Länder mit nicht-angemessenem Datenschutz die Rechtsabteilung zu kontaktieren.

8. Schulung von Mitarbeitenden und Überwachung von Auftragsbearbeitern

Alle Mitarbeitenden des Unternehmens, die Personendaten bearbeiten, werden über diese Richtlinie und den datenschutzkonformen Umgang mit Personendaten informiert bzw. geschult.

Darüber hinaus müssen mit allen Auftragsbearbeitern DPAs abgeschlossen werden (siehe obenstehend die Definition des Auftragsbearbeiters und seine Abgrenzung zum Verantwortlichen). Das Augenmerk ist dabei auf die Klauseln zur Datensicherheit (technische und organisatorische Massnahmen des Auftragsbearbeiters) inkl. Auditrechten des Unternehmens und der Genehmigungsregelung zum Beizug von Sub-Auftragsbearbeitern zu legen.

Mitarbeitende, die für die Überwachung anderer Mitarbeitender oder das Management der Beziehungen zu Auftragsbearbeitern zuständig sind, werden in Bezug auf die Überwachung dieser Mitarbeitenden und Auftragsbearbeiter geschult.

9. Melden einer Datensicherheitsverletzung

In **Anhang 1** findet sich die Weisung zur Meldung von Verletzungen der Datensicherheit. Darin sind Definitionen und verbindliche Handlungsschritte festgelegt. Das in **Anhang 1** enthaltene Formular ist in jedem Fall auszufüllen – auch wenn noch nicht abschliessend klar ist, ob überhaupt eine Datensicherheitsverletzung vorliegt.

10. Überwachung der Einhaltung und Durchsetzung der Vorschriften

Der **General Counsel** ist für die Verwaltung und Überwachung der Umsetzung dieser Richtlinie und für die Entwicklung verwandter Betriebsverfahren, Prozesse, Mitteilungen und Richtlinien zuständig.

Wenn Sie davon ausgehen, dass eine Bestimmung dieser Richtlinie oder einer damit zusammenhängenden Richtlinie, eines Betriebsverfahrens, Prozesses oder einer Weisung zum Schutz von Personendaten verletzt worden ist oder wird, wenden Sie sich bitte an die **Rechtsabteilung**.

Das Unternehmen wird regelmässige Überprüfungen und Audits durchführen, um die Einhaltung dieser Richtlinie zu überprüfen. Mitarbeitende, die gegen diese Richtlinie oder eine damit zusammenhängende Richtlinie, ein Betriebsverfahren oder Prozess zum Schutz von Personendaten verstossen, können disziplinarisch zur Verantwortung gezogen werden. Je nach Konstellation könnten sogar strafrechtliche Konsequenzen drohen.

11. Anhänge und weitere Richtlinien

Neben der vorliegenden Richtlinie sind auch die Anhänge 1 bis 3 sowie weitere Richtlinien des Unternehmens, welche die Personendatenbearbeitung betreffen, zu beachten und jederzeit einzuhalten:

- Richtlinie zur Informationssicherheit
- Weisung zur Meldung von Verletzungen der Datensicherheit (inkl. elektronisch ausfüllbarem Formular) (**Anhang 1**)
- Richtlinie zur Datenschutz-Folgenabschätzung (inkl. Fragebogen) (**Anhang 2**)
- Verhaltensregeln bei Auskunftsgesuchen inkl. Muster-Antwortbrief (**Anhang 3**)

Das Unternehmen behält sich vor, jederzeit neue Richtlinien zu erlassen. Die Mitarbeitenden werden in geeigneter Weise über den Erlass informiert.

12. Gültigkeits- und Dokumentenmanagement

Diese Richtlinie ist gültig ab dem 1. Mai 2024.

Frühere Versionen dieser Richtlinie werden grundsätzlich für einen Zeitraum von 10 Jahren aufbewahrt.