HIAG

Richtlinie der HIAG Gruppe zum Datenschutz

1. Juli 2020

1. Zweck

Die HIAG Immobilien Holding AG (das "**Unternehmen**") hat diese Richtlinie zur Regelung des Umgangs mit den personenbezogenen Daten von Kunden und Mitarbeitern des Unternehmens erlassen. Der Begriff "Unternehmen" umfasst alle Tochtergesellschaften des Unternehmens. Der Verlust personenbezogener Daten kann zu erheblichen Schäden für Einzelpersonen führen, einschliesslich Offenlegung heikler Daten, Unannehmlichkeiten und betrügerischer Nutzung der Informationen. Der Schutz der Vertraulichkeit und Integrität personenbezogener Daten 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 personenbezogenen Daten und sensiblen personenbezogenen Daten.
- Die Festlegung allgemeiner Grundsätze für den Schutz personenbezogener Daten.
- Die Regelung der Verantwortlichkeit für den Schutz personenbezogener Daten.

2. Umfang

Diese Richtlinie gilt für alle Mitarbeiter des Unternehmens ("**Sie**"), Agenten und Vertreter, einschliesslich aller Auftragnehmer oder Drittanbieter von Dienstleistungen für das Unternehmen ("**Drittdienstleister**"), die Zugang zu personenbezogenen Daten haben, die das Unternehmen erhoben hat oder anderweitig in ihrem Besitz hat. Diese Richtlinie gilt für alle personenbezogenen Daten, die vom Unternehmen erhoben, verwaltet, übertragen, gespeichert, aufbewahrt oder anderweitig verwendet werden, unabhängig davon, auf welchen Medien diese Informationen gespeichert sind und ob sie sich auf Mitarbeiter, Kunden oder andere Personen beziehen.

3. Definitionen

"Betroffener" bezeichnet eine identifizierte oder identifizierbare natürliche Person, über die personenbezogene Daten erhoben werden.

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

"Personenbezogene Daten" sind alle Informationen über eine identifizierte oder identifizierbare natürliche Person. Eine identifizierbare 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-Kenn-

zeichner 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;
- Staatlich vergebene Identifikationsnummern;
- Benutzerpasswörter oder PINs;
- Benutzeridentifikation und Zugangsdaten für das Konto, Passwörter, PINs und Antworten auf Sicherheitsfragen;
- Bankkontonummern;
- Geolokalisierungsdaten; und
- biometrische, medizinische, gesundheitliche oder krankenversicherungstechnische Informationen.

"Sensible personenbezogene Daten" sind personenbezogene Daten, die bei Verlust, Gefährdung, Zugriff oder unsachgemässer Weitergabe zu Schäden, peinlichen Situationen, Unannehmlichkeiten oder Ungerechtigkeiten für eine Person führen können und die daher einem erhöhten Schutz unterliegen. Beispiele für sensible personenbezogene Daten sind unter anderem:

- die von den Behörden ausgestellte Identifikationsnummer einer Person, einschliesslich einer Sozialversicherungsnummer, eines Führerscheins oder einer staatlich ausgestellten Identifikationsnummer;
- eine Bankkontonummer, Kreditkartennummer oder Debitkartennummer mit oder ohne erforderlichen Sicherheitscode, Zugangscode, persönliche Identifikationsnummer oder Passwort, die den Zugang zum Bankkonto einer Person ermöglichen würde;
- biometrische, medizinische, gesundheitliche oder krankenversicherungstechnische Informationen;
- religiöse oder philosophische Überzeugungen oder politische Meinungen;
- Gewerkschaftsmitgliedschaft;

- sexuelle Orientierung; und
- Strafregistereinträge.

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

"Sicherheitsvorfall" bezeichnet jede Handlung oder Unterlassung, welche die Sicherheit, Vertraulichkeit oder Integrität personenbezogener Daten oder die physischen, technischen, administrativen oder organisatorischen Sicherheitsvorkehrungen, die das Unternehmen oder ein Drittdienstleister zum Schutz personenbezogener Daten getroffen hat, beeinträchtigt. Der Verlust oder der unbefugte Zugriff auf, die unbefugte Offenlegung oder der unbefugte Erwerb von personenbezogenen Daten sind Sicherheitsvorfälle.

"Verantwortlicher" ist die natürliche oder juristische Person, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt.

"Verarbeitung" bezeichnet jeden Vorgang oder jede Reihe von Vorgängen, die mit personenbezogenen Daten mit oder ohne automatisiertem oder nicht automatisiertem Verfahren durchgeführt werden, wie z.B. Erhebung, Aufzeichnung, Organisation, Strukturierung, Speicherung, Anpassung oder Änderung, Abruf, Konsultation, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder anderweitige Bereitstellung, Anpassung oder Kombination, Einschränkung, Löschung oder Zerstörung.

4. Verwendung, Verarbeitung und Speicherung personenbezogener Daten

4.1 Faire und rechtmässige Verarbeitung

4.1.1 Im Allgemeinen

Wann immer das Unternehmen personenbezogene Daten verarbeitet, muss das Unternehmen sicherstellen, dass die Verarbeitung rechtmässig, fair und transparent in Bezug auf die betroffene Person erfolgt.

Für bestimmte Verarbeitungsvorgänge fungiert das Unternehmen als Datenverantwortlicher, gemeinsamer Datenverantwortlicher oder für andere als Datenverarbeiter. Wenn das Unternehmen als Datenverantwortlicher tätig ist, muss das Unternehmen sicherstellen, dass es über einen rechtmässigen Grund für die Erhebung und Verarbeitung personenbezogener Daten verfügt.

Wenn das Unternehmen als Datenverarbeiter tätig ist, verarbeitet das Unternehmen im Allgemeinen personenbezogene Daten im Namen seiner Kunden. In diesen Fällen ist der

Kunde dafür verantwortlich, eine Rechtsgrundlage für die Verarbeitung zu schaffen. Die vertragliche Sorgfalt ist jedoch von entscheidender Bedeutung, und die Verantwortlichkeiten des Unternehmens sollten immer klar in den Vereinbarungen des Unternehmens mit den Kunden definiert sein.

4.1.2 Rechtsgrundlage

Für die Verarbeitung personenbezogener Daten ist eine Rechtsgrundlage erforderlich. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn mindestens eine der folgenden Rechtsgrundlagen zutrifft:

Einwilligung: Die Zustimmung ist die einfachste Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Wichtig zu beachten ist, dass die Zustimmung freiwillig, spezifisch, informiert und unmissverständlich erteilt werden muss. Die Zustimmung 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 Zustimmung zur Verarbeitung deutlich erkennbar ist. Schweigen, vorgemerkte Kästchen oder Inaktivität gelten nicht als Zustimmung. Wann immer Unternehmen sensible personenbezogene Daten verarbeiten, ist eine ausdrückliche Zustimmung der betroffenen Person erforderlich. Die Zustimmung kann jederzeit widerrufen werden, und der Widerruf der Zustimmung sollte so einfach wie die Erteilung der Zustimmung möglich sein.

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 Erhebung von Daten

Es gehört zu den Grundsätzen des Unternehmens, dass es, wenn es personenbezogene Daten für einen bestimmten Zweck, einschliesslich für Personal- oder Beschäftigungszwecke, sammelt, die betroffene Person darüber informieren muss, wie es diese personenbezogenen Daten verwenden, verarbeiten, offenlegen, schützen und aufbewahren wird, indem es der Person zum Zeitpunkt der Bereitstellung der personenbezogenen Daten eine Datenschutzerklärung oder einen Datenschutzhinweis vorlegt. Sie dürfen personenbezogene Daten nur in Übereinstimmung mit den geltenden Unternehmensrichtlinien, Mitteilungen und der Zustimmung des Betroffenen sammeln, und die gesammelten personenbezogenen Daten 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.

4.3 Zugang, Nutzung und Weitergabe personenbezogener Daten

Sie dürfen nur dann auf personenbezogene Daten 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 personenbezogene Daten zugreifen. Sie dürfen personenbezogene Daten nicht in einer Weise verwenden, die mit der Mitteilung an die betroffene Person 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 personenbezogene Daten nur dann an einen anderen Mitarbeiter, Agenten oder Vertreter des Unternehmens weitergeben, wenn der Empfänger ein berufsbedingtes Bedürfnis hat, die Informationen zu kennen. Personenbezogene Daten dürfen nur dann an einen Drittdienstleister weitergegeben werden, wenn dieser die Informationen für die Erbringung der vertraglich vereinbarten Dienstleistungen kennen muss und wenn die Weitergabe der personenbezogenen Daten mit den Datenschutzhinweisen für die betroffene Person übereinstimmt.

4.4 Richtigkeit

Sie dürfen nur personenbezogene Daten erheben, pflegen und verwenden, die korrekt, vollständig und relevant für die Zwecke sind, für die sie erhoben wurden.

4.5 Sicherheit

Sie sind für den Schutz personenbezogener Daten verantwortlich. Das Unternehmen hat eine Informationssicherheitsrichtlinie implementiert, die technische, administrative und physische Sicherheitsvorkehrungen für den Schutz personenbezogener Daten festlegt. Sie

müssen die in der Informationssicherheitsrichtlinie festgelegten Sicherheitsverfahren jederzeit einhalten. Sie müssen besondere Sorgfalt walten lassen, um sensible personenbezogene Daten vor Verlust, unbefugtem Zugriff und unbefugter Weitergabe zu schützen.

4.6 Verantwortlichkeit

Wann immer das Unternehmen als Datenverantwortlicher tätig ist, muss es in der Lage sein, die Einhaltung der Grundsätze des Schutzes personenbezogener Daten im Sinne der DSGVO und anderer geltender Datenschutzgesetze nachzuweisen. Als Organisation wird das Unternehmen die aktuellen Praktiken bewerten und eine angemessene Führungsstruktur für den Schutz personenbezogener Daten entwickeln. Das Unternehmen hat eine Bestandsaufnahme personenbezogener Daten erstellt und geeignete organisatorische und technische Massnahmen ergriffen, um die Einhaltung der Grundsätze des Schutzes personenbezogener Daten sicherzustellen. Alle Mitarbeiter, Agenten und Vertreter, einschliesslich aller Auftragnehmer oder Drittanbieter, werden sich an diesen Grundsatz halten, indem sie geeignete Zustimmungen einholen, die Verfahren zur Meldung von Vorfällen einhalten (die Meldung kann in Absprache mit der Rechtsabteilung erfolgen) und jede neue Verarbeitung personenbezogener Daten zur Beurteilung (Privacy Impact Assessment, siehe unten) einreichen, bevor sie damit beginnen.

4.7 Transparenz

Bei der Verarbeitung personenbezogener Daten muss das Unternehmen transparent sein. Die Transparenz bezieht sich auf das Recht der betroffenen Person, die Kontrolle über ihre personenbezogenen Daten zu behalten, und verpflichtet das Unternehmen, die nötigen Massnahmen zu ergreifen, um sicherzustellen, dass die erforderlichen Informationen an die betroffene Person weitergegeben werden. Die betroffene Person ist darüber zu informieren:

- wer der Datenverantwortliche ist;
- die Quelle der Daten; Zwecke der Verarbeitung; Rechtsgrundlage und Interessen des Inhabers oder Dritter, soweit relevant;
- ob die Bereitstellung personenbezogener Daten eine Anforderung ist, warum und was sind die Folgen der Nichtbereitstellung?
- Empfänger oder deren Kategorien;
- Aufbewahrungsfristen oder, wenn nicht möglich, Kriterien für deren Bestimmung;
- Rechte der betroffenen Personen;
- Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen, einschliesslich geeigneter Schutzvorkehrungen.

Letztendlich bedeutet transparentes Handeln, dass das Unternehmen dem Betroffenen alle Informationen im Zusammenhang mit der Verarbeitung 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 Verarbeitung aufmerksam machen. Wann immer personenbezogene Daten über die Website des Unternehmens erhoben werden, werden diese Informationen in Form einer Datenschutzerklärung weitergegeben (siehe Abschnitt 4.2).

4.8 Rechte der Betroffenen Personen

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

4.8.1 Vorrang der Gesetzlichen und Vertraglichen Anforderungen

Obwohl die DSGVO den betroffenen Personen eine Reihe von wesentlichen Rechten zugesprochen hat, ist es wichtig zu beachten, dass diese Rechte nicht absolut sind und dass gesetzliche oder vertragliche Anforderungen Vorrang vor den Rechten der betroffenen Person haben können.

4.8.2 Recht auf Auskunft und Berichtigung

Jede Person hat das Recht festzustellen, ob die sie betreffenden personenbezogenen Daten verarbeitet werden oder nicht. Sie haben auch das Recht, eine Kopie der personenbezogenen Daten und zusätzliche Informationen über die Verarbeitung zu erhalten (siehe Abschnitt 4.8.6, Transparenz). Insbesondere ist das Unternehmen verpflichtet, die betroffenen Personen auf das Bestehen zusätzlicher Rechte, wie z.B. das Recht auf Löschung und Widerspruch, hinzuweisen.

Stellt eine betroffene Person Fehler in den zu verarbeitenden personenbezogenen Daten fest, hat sie das Recht auf unverzügliche und kostenlose Berichtigung der Daten. Ebenso hat die betroffene Person das Recht, die personenbezogenen Daten zu vervollständigen, wenn sie unvollständig sind. Handelt das Unternehmen als Datenverantwortlicher, liegt es in der Verantwortung des Unternehmens, angemessene Massnahmen zu ergreifen, um die Geltendmachung dieser Rechte zu erleichtern. Stellt eine betroffene Person einen Antrag auf Zugang zu ihren personenbezogenen Daten, so ist dieser innerhalb eines Monats nach Erhalt des schriftlichen Antrags zu erfüllen.

4.8.3 Recht auf Löschung ("Recht auf Vergessenwerden")

Eine betroffene Person hat das Recht vom Datenverantwortlichen zu verlangen, ihre personenbezogenen Daten zu löschen und nicht mehr zu verarbeiten. Diese Anfrage kann gestellt werden, weil (i) die Verarbeitung im Hinblick auf den Zweck, für den die personenbezogenen Daten erhoben werden, nicht mehr erforderlich ist oder (ii) die betroffene Person von ihrem Recht auf Widerruf Gebrauch gemacht hat oder (iii) die personenbezogenen Daten unrechtmässig verarbeitet werden oder (iv) die Löschung gesetzlich vorgeschrieben ist.

Wenn das Unternehmen als Datenverantwortlicher tätig ist und personenbezogene Daten veröffentlicht hat, muss das Unternehmen jeden, dem das Unternehmen die personenbezogenen Daten mitgeteilt hat, über diesen Antrag auf Löschung informieren, es sei denn, dies wäre unmöglich oder mit unverhältnismässigem Aufwand verbunden oder das Unternehmen macht einen Rechtsanspruch geltend, übt diesen aus oder verteidigt ihn.

4.8.4 Widerspruchsrecht

Das Widerspruchsrecht ist eng mit dem Recht auf Vergessenwerden verbunden und ähnelt diesem. Jede betroffene Person hat das Recht, dem Direktmarketing jederzeit zu widersprechen (Abbestellen). In diesem Fall ist das Unternehmen verpflichtet, die Verwendung der personenbezogenen Daten für Marketingzwecke einzustellen. Das Widerspruchsrecht kann auch in den Fällen ausgeübt werden, für die das Recht auf Vergessen gegeben ist.

4.8.5 Recht auf Datenübertragbarkeit

Das Unternehmen muss der Aufforderung eines Betroffenen nachkommen, ihm eine Kopie seiner personenbezogenen Daten zur Verfügung zu stellen. Dabei muss das Unternehmen sicherstellen, dass dies in einer strukturierten und allgemein üblichen Weise geschieht. Das Unternehmen muss auch sicherstellen, dass die Daten in einem maschinenlesbaren Format abgerufen werden können. Zweck dieses Rechts ist es, dem Betroffenen zu ermöglichen, seine personenbezogenen Daten an einen anderen Verantwortlichen zu übermitteln.

4.8.6 Transparenz

Es sei noch einmal betont, dass die im Rahmen der DSGVO erforderliche grössere Transparenz bedeutet, dass der Einzelne klar über das Bestehen seiner Rechte informiert werden muss.

4.8.7 Marketing

Wenn sich die betroffenen Personen auf der Website des Unternehmens registrieren oder sich für Marketingmaterial anmelden, erklären sie sich damit einverstanden, E-Mails oder andere Mitteilungen vom Unternehmen zu erhalten, die sie über die Dienstleistungen des

Unternehmens, zukünftige Ereignisse und andere Aktivitäten des Unternehmens, von denen sie glauben, dass sie für sie von Interesse sein werden, informieren.

In der Regel sollte das Unternehmen sicherstellen, dass alle seine Marketingaktivitäten (i) auf der Grundlage einer Einwilligung erfolgen, (ii) klar angeben, zu welchem Zweck die Daten einer betroffenen Person verwendet werden, (iii) den betroffenen Personen eine einfache Möglichkeit bieten, sich gegen die Einwilligung bzw. für die Abmeldung von Marketingbotschaften zu entscheiden und (iv) über ein Verfahren zur Bearbeitung von Beschwerden verfügen.

4.8.8 Weitere Informationen zu den Rechten der Betroffenen Personen

Sie müssen die geltenden Gesetze in Bezug auf die Rechte der betroffenen Personen einhalten. Wenn Sie sich nicht sicher sind, welche gesetzlichen Anforderungen gelten, oder wenn Sie eine Anfrage oder Beschwerde von einer betroffenen Person bezüglich der Verarbeitung ihrer personenbezogenen Daten erhalten, wenden Sie sich bitte an die Rechtsabteilung.

5. Datenschutz-Folgenabschätzung

Vor der Einführung eines neuen Systems oder Geschäftsprozesses mit personenbezogenen Daten sollte eine Folgenabschätzung zum Datenschutz durchgeführt werden (siehe Datenschutzrichtlinie). Der Zweck der Datenschutz-Folgenabschätzung besteht darin, die Art und Weise zu bewerten, wie ein System oder Geschäftsprozess personenbezogene Daten erhebt, verwendet, speichert, überträgt und löscht.

Ziel der Datenschutz-Folgenabschätzung ist es, potenzielle Vertraulichkeits- oder Datenschutzrisiken im System oder Geschäftsprozess zu identifizieren und alternative Wege für die Verarbeitung personenbezogener Daten zu prüfen und zu bewerten, um diese Risiken zu verringern.

6. Aufbewahrung und Löschung

In der Regel sollten alle gesammelten personenbezogenen Daten, die nicht mehr zur Erreichung des Zwecks der Verarbeitung erforderlich sind, dauerhaft gelöscht werden, es sei denn, für die fraglichen personenbezogenen Daten gilt eine gesetzliche Aufbewahrungsfrist oder es gibt einen anderen legitimen Grund zu deren Speicherung. Um dieser Anforderung gerecht zu werden, sollte das Unternehmen (i) maximale Aufbewahrungsfristen für alle gesammelten personenbezogenen Daten und (ii) regelmässige Überprüfungsprozesse zusammen mit Mechanismen zur Bereinigung personenbezogener Daten einführen.

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. Sie müssen die geltenden Zeitpläne und Richtlinien zur Aufbewahrung von Aufzeichnungen befolgen und alle Datenträger, die personenbezogene Daten enthalten, in Übereinstimmung mit den geltenden Richtlinien zur Entsorgung von Aufzeichnungen, falls vorhanden, vernichten.

7. Internationale Datenübermittlung

In einigen Fällen kann das Unternehmen personenbezogene Daten an Empfänger weitergeben, die ihren Sitz in Ländern ausserhalb der Europäischen Union und der Schweiz haben, deren Gesetze möglicherweise nicht das gleiche Schutzniveau für personenbezogene Daten bieten. In solchen Fällen wird das Unternehmen sicherstellen, dass es angemessene Sicherheitsvorkehrungen gibt, die den gesetzlichen Verpflichtungen des Unternehmens zum Schutz personenbezogener Daten entsprechen. Der angemessene Schutz kann eine Vereinbarung über die Übermittlung personenbezogener Daten mit dem Empfänger sein, die auf Standardvertragsklauseln basiert, die von der Europäischen Kommission für die Übermittlung personenbezogener Daten in Drittländer genehmigt worden sind, oder das Abstützen auf den sogenannten Privacy Shield.

8. Schulung von Mitarbeitern und Überwachung von Auftragnehmern

Alle Mitarbeiter des Unternehmens, die Zugang zu personenbezogenen Daten haben, müssen über diese Richtlinie und den Umgang mit personenbezogenen Daten informiert und geschult werden. Darüber hinaus muss, wenn personenbezogene Daten einem Drittdienstleister anvertraut werden, eine ordnungsgemässe Instruktion des Drittdienstleisters und die Aufsicht über seinen Umgang mit diesen personenbezogenen Daten durch entsprechende Verträge gewährleistet sein. Mitarbeiter, die für die Überwachung anderer Mitarbeiter oder das Management der Beziehungen zu Drittdienstleistern verantwortlich sind, müssen in Bezug auf die Überwachung dieser Mitarbeiter und Drittdienstleister geschult werden.

9. Melden eines Sicherheitsvorfalls

Wenn Sie wissen oder vermuten, dass ein Sicherheitsvorfall aufgetreten ist, versuchen Sie nicht, die Angelegenheit selbst zu untersuchen. Wenden Sie sich umgehend an den General Counsel. Sie sollten alle Beweise im Zusammenhang mit dem potenziellen Sicherheitsvorfall aufbewahren.

10. Überwachung der Einhaltung und Durchsetzung der Vorschriften

Der General Counsel ist verantwortlich für die Verwaltung und Überwachung der Umsetzung dieser Richtlinie und gegebenenfalls für die Entwicklung verwandter Betriebsverfahren, Prozesse, Richtlinien, Mitteilungen und Richtlinien. Wenn Sie davon ausgehen, dass

eine Bestimmung dieser Richtlinie oder einer damit zusammenhängenden Richtlinie, eines Betriebsverfahrens, Prozesses oder einer Weisung zum Schutz personenbezogener Daten 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. Mitarbeiter, die gegen diese Richtlinie und alle damit zusammenhängenden Richtlinien, Betriebsverfahren oder Prozesse zum Schutz personenbezogener Daten und zur Umsetzung dieser Richtlinie verstossen, können disziplinarisch zur Verantwortung gezogen werden.

11. Verwandte Richtlinien

Auch andere Unternehmensrichtlinien beziehen sich auf die Erfassung, Verwendung, Speicherung, den Schutz und die Verarbeitung personenbezogener Daten und können für die Umsetzung dieser Richtlinie relevant sein. Sie sollten sich mit diesen Richtlinien vertraut machen, einschliesslich:

- Richtlinie zur Informationssicherheit
- Richtlinie betreffend Meldung von Datenschutzverletzungen (Anhang 1)
- Richtlinie zur Datenschutz-Folgenabschätzung für Systeme und Prozesse (Anhang 2)
- Verfahrensregeln für den Antrag einer betroffenen Person auf Zugang zu personenbezogenen Daten (Anhang 3)

12. Gültigkeits- und Dokumentenmanagement

Diese Richtlinie ist gültig ab dem 1. Juli 2020.

Frühere Versionen dieser Richtlinie müssen für einen Zeitraum von 5 Jahren aufbewahrt werden, sofern durch gesetzliche oder vertragliche Bestimmungen nichts anderes bestimmt ist.

HIAG

Anhang 1 – Richtlinie betreffend Meldung von Datenschutzverletzungen

1. Zweck

Das Unternehmen unternimmt alle Anstrengungen, personenbezogene Daten vor versehentlichen oder vorsätzlichen Sicherheitsvorfällen zu schützen, um eine Datenschutzverletzung zu vermeiden, welche die Sicherheit beeinträchtigen könnte.

Einschränkungen der Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen können zu Schäden von Einzelpersonen, Reputationsschäden, nachteiligen Auswirkungen auf die Erbringung von Dienstleistungen, Gesetzesverstössen und Kosten führen.

Diese Richtlinie legt das Verfahren fest, das zu befolgen ist, um sicherzustellen, dass Datenschutzverletzungen und Sicherheitsvorfälle im gesamten Unternehmen effektiv und einheitlich gehandhabt werden.

Diese Richtlinie betreffend Meldung von Datenschutzverletzungen bezieht sich auf alle personenbezogenen Daten und sensiblen personenbezogenen Daten des Unternehmens, unabhängig davon, in welcher Form die Daten vorhanden sind.

Das Ziel dieser Richtlinie betreffend Meldung von Datenschutzverletzungen ist es, Verstösse einzudämmen, das mit einer Verletzung verbundene Risiko zu minimieren und zu prüfen, welche Massnahmen erforderlich sind, um personenbezogene Daten zu schützen und weitere Verstösse zu verhindern.

Für die Zwecke dieser Richtlinie betreffend Meldung von Datenschutzverletzungen umfassen Sicherheitsvorfälle sowohl bestätigte als auch vermutete Vorfälle.

2. Arten von Verstössen

Ein Sicherheitsvorfall im Zusammenhang mit dieser Richtlinie betreffend Meldung von Datenschutzverletzungen sind Ereignisse oder Massnahmen, welche die Vertraulichkeit, Integrität oder Verfügbarkeit von Systemen oder Daten aus Versehen oder vorsätzlich gefährden können und welche die Datenbestände und den Ruf des Unternehmens geschädigt haben oder schädigen könnten.

Ein Sicherheitsvorfall beinhaltet, ist aber nicht beschränkt auf Folgendes:

- Verlust oder Diebstahl vertraulicher oder sensibler Daten oder Geräte, auf denen diese Daten gespeichert sind (z.B. Verlust von Laptop, USB-Stick, iPad / Tablet PC oder Papierdatensatz);
- Diebstahl oder Ausfall von Geräten;
- Systemfehler;

- unbefugte Nutzung, unbefugter Zugriff oder unbefugte Änderung von Daten oder Informationssystemen;
- Versuche (fehlgeschlagen oder erfolgreich), sich unbefugten Zugriff auf Informationen oder IT-Systeme zu verschaffen;
- unbefugte Weitergabe sensibler / vertraulicher Daten;
- Verunstaltung der Website;
- Hackerangriffe;
- unvorhergesehene Umstände wie ein Brand oder eine Überschwemmung;
- menschliches Versagen;
- Straftaten, bei denen Informationen durch Täuschung des Unternehmens, das sie besitzt, erhalten werden.

3. Meldung eines Vorfalls

Jeder, der auf die Informationen des Unternehmens zugreift, diese verwendet oder verwaltet, ist dafür verantwortlich, Datenverstösse und Sicherheitsvorfälle unverzüglich dem Datenschutzbeauftragten ("**DSB**") zu melden. Tritt die Verletzung auf oder wird sie ausserhalb der normalen Arbeitszeit festgestellt, so ist sie so schnell wie möglich zu melden. Der Bericht muss vollständige und genaue Angaben über den Vorfall, den Zeitpunkt der Verletzung (Datum und Uhrzeit), den Meldenden, ob sich die Daten auf Personen beziehen, die Art der Informationen und die Anzahl der beteiligten Personen enthalten. Dazu sollte das Formular zur Meldung von Vorfällen ausgefüllt werden (enthalten im Anhang zu dieser Richtlinie betreffend Meldung von Datenschutzverletzungen).

Sie sollten sich bewusst sein, dass jeder Verstoss gegen die Datenschutzbestimmungen dazu führen kann, dass ein unternehmensinternes Disziplinarverfahren eingeleitet wird.

4. Eindämmung und Wiederherstellung

Der DSB wird zunächst feststellen, ob die Verletzung noch immer vorliegt. In diesem Fall werden unverzüglich geeignete Massnahmen ergriffen, um die Auswirkungen des Verstosses zu minimieren.

Der DSB wird in Verbindung mit den zuständigen Mitarbeitern eine erste Bewertung vornehmen, um die Schwere des Verstosses festzustellen und festzustellen, wer die Leitung der Untersuchung des Verstosses übernehmen wird (dies hängt von der Art des Verstosses ab; in einigen Fällen könnte es auch der DSB selber sein).

Der Leiter der Untersuchung wird feststellen, ob etwas getan werden kann, um Datenverluste rückgängig zu machen und den Schaden zu begrenzen, den die Verletzung verursachen könnte.

Der Leiter der Untersuchung stellt fest, wer im Rahmen der ersten Massnahmen zur Schadensbegrenzung benachrichtigt werden muss, und informiert gegebenenfalls die Polizei.

Um einen Vorfall effizient zu behandeln, kann Rat von Experten aus dem gesamten Unternehmen eingeholt werden.

Der Leiter der Untersuchung legt in Verbindung mit dem/den zuständigen Mitarbeitern fest, welche geeigneten Massnahmen zu ergreifen sind, um eine Lösung des Vorfalls zu gewährleisten.

5. Untersuchung und Risikobewertung

Der Leiter der Untersuchung führt die Untersuchung unverzüglich und nach Möglichkeit innerhalb von 24 Stunden nach Entdeckung / Meldung der Verletzung durch.

Der Leiter der Untersuchung wird die Verletzung untersuchen und die damit verbundenen Risiken bewerten, z.B. die möglichen negativen Folgen für den Einzelnen, wie schwerwiegend oder substanziell diese sind und wie wahrscheinlich sie sind.

Bei der Untersuchung müssen die folgenden Punkte berücksichtigt werden:

- die Art der betroffenen Daten;
- wie sensibel die betroffenen Daten sind;
- die vorhandenen Schutzmassnahmen (z.B. Verschlüsselungen);
- was mit den Daten passiert ist (z.B. Verlust oder Diebstahl);
- ob die Daten zu einer illegalen oder unangemessenen Verwendung genutzt werden können;
- von der Verletzung betroffene Person(en), Anzahl der beteiligten Personen und die möglichen Auswirkungen auf diese Person(en);
- ob der Verstoss weiterreichende Folgen hat.

6. Benachrichtigung

Der Leiter der Untersuchung oder der DSB wird in Absprache mit den zuständigen Kollegen feststellen, ob die Datenschutzbehörde über den Verstoss informiert werden muss, und wenn ja, sie soweit möglich innerhalb von 72 Stunden nach Bekanntwerden des Verstosses informieren.

Jeder Vorfall wird von Fall zu Fall bewertet, jedoch müssen die folgenden Punkte berücksichtigt werden:

- ob die Verletzung wahrscheinlich zu einem hohen Risiko führt, die Rechte und Freiheiten des Einzelnen gemäss den Datenschutzbestimmungen zu beeinträchtigen;
- ob die Meldung der/den betroffenen Person(en) helfen würde (z.B. könnten sie auf die Informationen reagieren, um Risiken zu minimieren?);
- ob die Benachrichtigung dazu beitragen würde, die unbefugte oder rechtswidrige Verwendung personenbezogener Daten zu verhindern;
- ob gesetzliche / vertragliche Meldepflichten bestehen;
- die Gefahren einer unnötigen Benachrichtigung. Nicht jeder Vorfall rechtfertigt eine Benachrichtigung und eine unnötige Benachrichtigung kann zu unverhältnismässigen Anfragen und Arbeiten führen.

Personen, deren personenbezogene Daten vom Vorfall betroffen sind und bei denen angenommen werden kann, dass ihre Rechte und Freiheiten durch den Vorfall mit hoher Wahrscheinlichkeit beeinträchtigt werden, werden unverzüglich informiert. Die Benachrichtigung enthält eine Beschreibung, wie und wann die Verletzung stattgefunden hat und die durch den Vorfall betroffenen Daten. Es werden konkrete und klare Ratschläge gegeben, was sie tun können, um sich selbst zu schützen, und es wird dargelegt, welche Massnahmen bereits ergriffen worden sind, um die Risiken zu mindern. Den Personen wird auch eine Möglichkeit geboten, sich mit dem Unternehmen in Verbindung zu setzen, um weitere Informationen zu erhalten oder Fragen zu den Ereignissen zu stellen.

Der Leiter der Untersuchung oder der DSB muss prüfen, ob Dritte wie Polizei, Versicherer, Banken oder Kreditkartenunternehmen und Gewerkschaften zu informieren sind. Dies könnte der Fall sein, wenn eine illegale Handlung vorliegt oder vorliegen könnte, oder wenn die Gefahr besteht, dass in Zukunft illegale Handlungen stattfinden könnten.

Der Leiter der Untersuchung oder der DSB muss prüfen, ob die Kommunikationsabteilung zu informieren ist im Hinblick auf eine allfällige Pressemitteilung oder Medienanfragen.

Über jede Verletzung personenbezogener Daten wird ein Protokoll geführt, unabhängig davon, ob eine Benachrichtigung erforderlich war oder nicht.

7. Bewertung und Reaktion

Sobald der Vorfall unter Kontrolle ist, führt der DSB eine vollständige Überprüfung der Ursachen der Verletzung, der Wirksamkeit der Reaktion(en) und der Frage durch, ob Änderungen an Systemen, Richtlinien und Verfahren vorgenommen werden sollten.

Bestehende Kontrollen werden überprüft, um ihre Angemessenheit festzustellen und festzustellen, ob Korrekturmassnahmen ergriffen werden sollten, um das Risiko des Auftretens ähnlicher Vorfälle zu minimieren.

Bei der Überprüfung wird berücksichtigt:

- wo und wie personenbezogene Daten aufbewahrt werden und wo und wie sie gespeichert werden;
- wo die grössten Risiken liegen, einschliesslich der Identifizierung potenzieller Schwachstellen im Rahmen bestehender Sicherheitsvorkehrungen;
- ob die Übertragungsverfahren sicher sind; welche Daten mindestens ausgetauscht werden müssen;
- Sensibilisierung der Mitarbeiter;
- Umsetzung von Handlungsanweisungen bei Datenverletzungen und Identifizierung eines Teams, das für die Intervention bei gemeldeten Sicherheitsverletzungen verantwortlich ist.

Falls notwendig, wird der General Counsel einen Bericht, der Änderungen an Systemen, Richtlinien und Verfahren empfiehlt, prüfen.

8. Änderung und Überarbeitung

Diese Richtlinie betreffend Meldung von Datenschutzverletzungen kann von Zeit zu Zeit überarbeitet und ergänzt werden.

MELDEFORMULAR FÜR DATENSCHUTZVERLETZUNGEN

Bitte melden Sie Datenschutzverletzungen umgehend. Wenn Sie eine Datenschutzverletzung feststellen, informieren Sie bitte den Datenschutzbeauftragten und füllen Sie Abschnitt 1 dieses Formulars aus und senden Sie es per E-Mail an den Datenschutzbeauftragten.

Abschnitt 1: Mitteilung der Datenschutzverletzung	Von der meldenden Person auszufüllen
Datum der Entdeckung des Vorfalls:	
Datum/Daten des Vorfalls:	
Ort des Vorfalls:	
Name der Person, die den Vorfall meldet:	
Kontaktdaten der Person, die den Vorfall meldet (E-Mail-Adresse, Telefonnummer):	
Kurze Beschreibung des Vorfalls oder Details der verlorenen Informationen:	
Anzahl der betroffenen Personen, falls bekannt:	
Wurden personenbezogene Daten gefährdet? Wenn ja, dann geben Sie bitte Details an:	
Kurze Beschreibung aller zum Zeitpunkt der Feststellung getroffenen Massnahmen:	
Zur Verwendung durch den Datenschutzbeauftragten	
Empfangen durch:	
Am (Datum):	
Weitergeleitet zur Weiterbehandlung an:	
Am (Datum):	
Kontaktdaten der Person, die den Vorfall meldet (E-Mail-Adresse, Telefonnummer):	

Abschnitt 2: Beurteilung der Schwere des Vorfalls	Vom Leiter der Untersuchung in Absprache mit der Person des von der Verletzung betroffenen Bereichs und ggf. der IT auszufüllen.

Details zu den IT-Systemen, Ausrüstungen, Geräten und Aufzeichnungen, die von der Sicherheitsverletzung betroffen sind:

Details zum Informationsverlust:

Was ist die Art der verlorenen Informationen?

Wie viele Daten sind verloren gegangen? Bei Verlust / Diebstahl des Laptops: Wann wurde der Laptop letztmals auf dem zentralen IT-System gesichert?

Sind die Informationen nur einmal vorhanden? Wird der Verlust nachteilige betriebliche, wissenschaftliche, finanzielle, rechtliche, haftungsrechtliche oder Reputationsfolgen für das Unternehmen oder Dritte haben?

Wie viele Personen sind betroffen?

Sind die Daten an vertragliche Sicherheitsvereinbarungen gebunden?

Was ist die Art der Sensibilität der Daten? Bitte geben Sie Einzelheiten zu allen Arten von Informationen an, die in eine der folgenden Kategorien fallen:

Persönliche Daten mit **hohem Risiko**

- Sensible personenbezogene Daten (wie in den Datenschutzbestimmungen definiert), die sich auf lebende, identifizierbare Personen beziehen.
    a) rassische oder ethnische Herkunft;

b) politische Meinungen oder religiöse Überzeugungen;
c) Gewerkschaftsmitgliedschaft;
d) Genetik;
e) Biometrie (bei Verwendung für Identifikationszwecke);
f) Gesundheit;
g) Sexualleben oder sexuelle Orientierung.

- Informationen, die zur Begehung von Identitätsbetrug verwendet werden könnten, wie z.B. persönliche Bankkonten und andere Finanzinformationen, nationale Identifikatoren, wie Kopien von Pässen und Visa;
- Personenbezogene Daten von schutzbedürftigen Erwachsenen und Kindern;
- Detaillierte Profile von Personen, einschliesslich Informationen über Arbeitsleistung, Gehälter oder das Privatleben, die dieser Person bei Bekanntgabe erheblichen Schaden oder Ärger verursachen würden;
- Sicherheitsinformationen, die bei Offenlegung die Sicherheit von Personen gefährden würden.

Es obliegt dem Datenschutzbeauftragten oder dem Leiter der Untersuchungen zu prüfen, ob der Vorfall an den General Counsel weitergeleitet werden soll.

Abschnitt 3: Getroffene Massnahmen	Durch den DSB oder den Leiter der Untersuchung auszufüllen
Vorfallnummer	e.g. Jahr/001
Bericht erhalten von:	
Am (Datum):	

Massnahmen des / der Verantwortlichen:	
Wurde der Vorfall der Polizei gemeldet?	Ja / Nein
Wenn JA, benachrichtigt am (Datum):	
Folgemassnahmen erforderlich / empfohlen:	
Berichtet an den DSB und den Leiter der Untersuchung am (Datum):	

HIAG

Anhang 2 – Richtlinie zur Datenschutz-Folgenabschätzung von Systemen und Prozessen

Neue Systeme und Prozesse können erfordern, dass Daten im Unternehmen verarbeitet, gespeichert und abgerufen oder im Namen des Unternehmens von externen Dienstleistern verwaltet werden. Die folgende Richtlinie zur Datenschutz-Folgenabschätzung wurde erstellt, um die verschiedenen Datenflüsse aufzuzeigen und zu dokumentieren, die durch ein neues System oder Verfahren entstehen können, und um sicherzustellen, dass alle anwendbaren Verpflichtungen zur Einhaltung des Datenschutzes erfüllt werden.

Für jedes dieser Systeme / Prozesse wird das Unternehmen mit den Verantwortlichen für die Systeme / die Prozesse zusammenarbeiten, um:

- zu klären, was das System / der Prozess beinhaltet;
- festzustellen, welche Auswirkungen dieses System / dieser Prozess hat, und eine Datenschutz-Folgenabschätzung unter Berücksichtigung der Datenschutzanforderungen des Unternehmens durchzuführen;
- geeignete Datenschutzmassnahmen für das System / den Prozess zu entwickeln und ihre Umsetzung sicherzustellen. Mögliche Massnahmen können unter anderem folgende sein:
    - Datenschutzhinweise für Systembenutzer;
    - Festlegung von Datenaufbewahrungsstandards für personenbezogene Daten, die im System verarbeitet werden, falls es keine solchen gibt;
    - Detaillierte Hintergrundanalyse und Anweisungen betreffend die vom Unternehmen benötigten Informationen;
    - Anweisungen für Systembenutzer.

Fragebogen zur Datenschutz-Folgenabschätzung

System / Prozess: (Bitte erläutern Sie die im Namenssystem verwendeten Abkürzungen)

Vorlage ergänzt durch:

(Bitte geben Sie den Namen der Person an, die diesen Fragebogen ausgefüllt hat, und auch den Namen des Systemverantwortlichen, falls dieser von der Person abweicht, die diesen Fragebogen ausgefüllt hat.)

Schritt Eins – Bewertung des aktuellen Systems / Prozesses

NB – Bitte stellen Sie sicher, dass Sie sich beim Ausfüllen des Fragebogens auf die vereinbarten Schlüsseldefinitionen beziehen, insbesondere in Bezug auf die Definition von "personenbezogenen Daten".

	Frage	Antwort / Erläuterungen / Risiken
	Angemessene und rechtmässige Verarbeitungsanforderungen	
1.	Werden personenbezogene Daten und vertrauliche Daten verarbeitet (siehe Definition der "personenbezogenen Daten" und "verarbeitet" in der HIAG-Datenschutzrichtlinie)	*Bitte nur mit "Ja" oder "Nein" antworten.*
2.	Werden sensible personenbezogene Daten verarbeitet? Wenn ja, listen Sie bitte die Datenklassen auf.	*Bitte mit "Ja" oder "Nein" antworten.* *Wenn Sie mit "Ja" antworten, geben Sie bitte die spezifischen Elemente der sensiblen personenbezogenen Daten an, die im System verarbeitet werden. "Sensible personenbezogene Daten" sind personenbezogene Daten einer Person, die aus Informationen über Folgendes bestehen* • *die rassische oder ethnische Herkunft der betroffenen Person,* • *ihre politischen und weltanschaulichen Ansichten,*

		• *ihre religiösen Überzeugungen und Aktivitäten oder andere Überzeugungen und Aktivitäten ähnlicher Art,* • *ob sie Mitglied einer Gewerkschaft ist und ihre Position in Gewerkschaften,* • *ihre körperliche oder geistige Gesundheit oder ihren Zustand,* • *ihr Sexualleben und ihre Privatsphäre,* • *ihre Verwaltungs- oder Strafverfahren und Verurteilungen,* • *ihre Sozialversicherungsunterlagen.* *Bitte geben Sie bei der Beantwortung dieser Frage auch an, ob das System über "Freitext"-Bereiche verfügt, in denen eine Person bei entsprechender Entscheidung sensible personenbezogene Daten eingeben kann.*
3.	Um welche Art von personenbezogenen Daten und vertraulichen Daten handelt es sich (Namen, Adressen, Kontaktdaten, Geschlecht, Krankengeschichte, Gehalts-/Leistungsdaten, etc.)? Bitte geben Sie eine Liste der Datenklassen / Kategorien für den Prozess / das System an. Wenn möglich, stellen Sie bitte ein Datenwörterbuch zur Verfügung.	*Personenbezogene Daten können unter anderem Folgendes umfassen:* • *Name (Vor- und Nachname)* • *E-Mail-Adresse* • *Kontaktdaten* • *Geschlecht* • *Geburtsdatum* • *Gehalt* • *Leistungsdaten* • *Ausbildung* • *Pass- oder ID-Daten* • *System-Login-Daten (Benutzername und Passwort)* *Wenn auch vertrauliche Informationen zur Kundenbindung im System verarbeitet werden, geben Sie bitte Details an.* *Bitte stellen Sie eine Excel- oder Word Zusammenstellung zur Verfügung, die alle Datenelemente enthält, die im System verarbeitet werden.*

4.	Woher stammen die personenbezogenen Daten – einschliesslich sensibler personenbezogener Daten und vertraulicher Daten? (Geben Sie Details zu anderen Prozessen / Systemen / Datenfeeds etc. an)	*Die Daten können von Unternehmen, Mitarbeitern oder Auftragnehmern direkt manuell in das System eingegeben werden.* *Die Daten können auch über einen Feed von einem oder mehreren der folgenden "Upstream"-Systeme in das System eingegeben werden:* *Die Daten können auch manuell von Kunden des Unternehmens oder anderen Dritten direkt in das System eingegeben werden.*
5.	Beschreiben Sie den Zweck der Verarbeitung und skizzieren Sie den Prozess, einschliesslich der Schlüsselelemente.	*Fassen Sie den Zweck des Systems in einem Satz zusammen und erweitern Sie dann Ihre Antwort, um weitere allgemeine Details über den Geschäftsbedarf für das System, den Zweck der Verarbeitung und einen Überblick über den Prozess (und ein Flussdiagramm, falls vorhanden) zu erhalten.* *Sie können Details über die geschäftlichen Anforderungen an das System und / oder den Zweck des Systems in den Einführungsabschnitten von PowerPoint-Präsentationen, Systemspezifikationsdokumenten, Lieferanten-RFPs oder Benutzerhandbüchern für das System finden. Sie sollten angeben, wer das System implementiert und welchen erwarteten Nutzen für das Unternehmen (z.B. höhere Umsätze oder Effizienzsteigerungen) Sie durch den Einsatz erzielen möchten.*
6.	Klären Sie, wessen Daten erfasst werden (Mitarbeiter, Auftragnehmer, Kunden, Lieferanten, Ex-Mitarbeiter usw. Das sind nur Beispiele und stellt keine vollständige Liste dar).	*Die personenbezogenen Daten, die im System verarbeitet werden, können sich auf einen oder mehrere der folgenden Punkte beziehen:* • *Mitarbeiter des Unternehmens* • *Auftragnehmer des Unternehmens* • *Ehemalige Auftragnehmer des Unternehmens* • *Kunden* • *Ehemalige Kunden* • *Lieferanten*

		• *Ehemalige Lieferanten* • *Andere (Details angeben)*
7.	Sind die betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten informiert?	*Die Antwort auf diese Frage wird wahrscheinlich eine der folgenden sein:* • *Nein* • *Ja, eine Datenschutzerklärung wird erstellt und im System zur Verfügung gestellt.* • *Ja, eine Datenschutzerklärung ist verfügbar (Hinweis: Bitte senden Sie uns eine Kopie zur Überprüfung).* • *Ja, die Kunden oder die Verkäufer haben die Pflicht, die betroffenen Personen zu benachrichtigen.* • *Ja, als Teil des Arbeitsvertrags oder des Personalhandbuchs.* • *Ja, andere (Details).*
8.	Was ist der Zweck, der den betroffenen Personen (siehe Definition unten) bei der Erhebung der personenbezogenen Daten mitgeteilt wird?	*Die Antwort auf diese Frage hängt von der Antwort auf Frage 7 ab.* *Aus der Datenschutzerklärung können die Nutzer des Systems entnehmen, dass der Zweck des Systems darin besteht, [den Zweck des Systems mit einem Satz zu wiederholen, wie in Frage 5 oben dargelegt].*
	Datenmanagement – d.h. Richtigkeit, Aufbewahrungsrichtlinien etc.	
9.	Wer (welche juristische Person) ist für das Datenmanagement verantwortlich?	*Die Antwort auf diese Frage wird wahrscheinlich eine der folgenden sein (bitte wählen Sie eine passende Antwort):* • *Ein externer Anbieter lizenziert das System an uns, und wir sind für das Datenmanagement verantwortlich.*
10.	Welche Verfahren gibt es für die Verwaltung der im System gespeicherten Daten? D.h. wer ist dafür verantwortlich, Zugang zu den Daten zu gewähren und sie auf dem neuesten Stand zu	*Geben Sie Details über den Prozess zur Gewährung von Benutzerzugriff auf das System an (z.B. welches benannte Team ist für die Gewährung von Benutzerzugriff auf das System verantwortlich - wie viele Personen sind in diesem Team und wo befinden sie sich?).*

	halten?	*Die Daten können im System durch eines oder mehrere der folgenden Verfahren auf dem neuesten Stand gehalten werden:* • *Durch Dateneinspeisungen aus vorgelagerten Systemen.* • *Manuell aktualisiert durch ein Mitglied des Engagement-Teams.* • *Wird von den Systemadministratoren manuell aktualisiert.* • *Manuelle Aktualisierung durch die Benutzer des Systems (Kunden, Unternehmen oder Dritte).* • *Die verarbeiteten Daten sind eine "Momentaufnahme" und werden nach dem Hochladen / nach Abschluss eines Auftrags nicht aktualisiert.* *Wie ist der Prozess zum Entzug von Zugriffsrechten, wenn der Zugriff nicht mehr benötigt wird (z.B. wenn ein Mitarbeiter uns verlässt oder in eine andere Rolle wechselt, für die kein Zugriff mehr erforderlich ist)?*
11.	Führt der Prozess zu einem zusätzlichen Prozess / System?	*Antworten Sie mit "Ja" oder "Nein".* *Wenn "Ja", geben Sie die Namen der nachgeschalteten Systeme an, aus denen dieses System versorgt wird, und geben Sie an, ob es sich um eine manuelle oder automatische Einspeisung handelt. Fügen Sie Einzelheiten zu allen Berichten hinzu, die Daten anzeigen, die im System verarbeitet werden.*
12.	Wie werden die personenbezogenen Daten verwendet? (Erklären Sie, wie die Richtigkeit der personenbezogenen Daten gewährleistet wird.)	*Sie haben den Zweck des Systems in Frage 5 oben näher erläutert. Erklären Sie nun, wie die im System verarbeiteten personenbezogenen Daten es uns ermöglichen, diesen Zweck zu erreichen. So können beispielsweise die personenbezogenen Daten im System verwendet werden, um Personen zu identifizieren, für die wir Dienstleistungen über das System erbringen.*
13.	Gibt es Abhängigkeiten von anderen Systemen / Prozessen? D.h. gibt es Änderungen in einer Datenbank, die automatisch zu Änderungen in einer anderen	*Geben Sie Details zu jeder automatischen Einspeisung von Daten (upstream oder downstream) aus dem System in einen zusätzlichen Prozess / ein zusätzliches System an.*

	führen?	
14.	Gibt es eine mit dem Prozess / System verbundene Datenaufbewahrungsrichtlinie? Wenn ja, geben Sie Details an, z.B. Aufbewahrungsfrist, Zugriffsrechte, Datenvernichtung etc.	*Geben Sie Einzelheiten zu den Verfahren oder Richtlinien für die Datenspeicherung und -entsorgung im System an, einschliesslich:* • *Angemessene Aufbewahrungsfrist / Richtlinie zur Aufbewahrung.* • *Verfahren zum Löschen von Daten (manuell oder automatisiert?)* • *Werden die Daten in einem separaten Archivsystem aufbewahrt, bevor sie dauerhaft gelöscht werden?* *Wenn es derzeit keine Datenaufbewahrungsrichtlinie für das System gibt, muss eine solche erstellt werden, um die Datenschutzgesetze einzuhalten.*
	Eigentum – Hard- und Software	
15.	Welche juristische Person besitzt das mit dem Prozess verbundene System?	*Die Antwort auf diese Frage wird wahrscheinlich eine der folgenden sein (bitte wählen Sie eine passende Antwort):* • *Das System wurde von uns selbst entwickelt und ist daher im Besitz von uns.*
16.	Besitzt dieselbe juristische Person die Hardware / Server usw. (Bitte geben Sie Details an.)'	*Die Antwort auf diese Frage wird wahrscheinlich eine der folgenden sein (bitte wählen Sie eine passende Antwort):* 1. *Das System wird innerhalb unserer Infrastruktur gehostet:* • *Rechenzentrum [Land]* • *Rechenzentrum [Land]* • *Rechenzentrum [Land]* 2. *Das System wird extern vom Anbieter oder seinem Drittanbieter gehostet [Geben Sie den Standort (Land, Stadt) an].*

17.	Wo sind die Server untergebracht, z.B. USA.	*Im Anschluss an Ihre Antwort auf die vorstehende Frage 16 wird die Antwort auf diese Frage wahrscheinlich eine der folgenden zwei sein:* 1. *Das Rechenzentrum in [Standort - Land und Stadt]; oder* 2. *Das Rechenzentrum des Anbieters in [Standort - Land und Stadt].*
	Datenübermittlung ins Ausland	
18.	Werden die personenbezogenen Daten ausserhalb des Unternehmens übermittelt?	*Antworten Sie mit "Ja" oder "Nein".* *Beachten Sie, dass, wenn wir das System hosten, jeder Zugriff externer Parteien auf personenbezogene Daten, die im System verarbeitet oder gespeichert werden, eine Übertragung der personenbezogenen Daten ausserhalb des Unternehmens darstellt und daher hier aufgeführt werden muss.*
19.	An wen werden die personenbezogenen Daten übermittelt? Einbeziehung aller externen Dritten, z.B. Regierungsstellen, Regulierungsbehörden, Datenverarbeiter usw.	*Wenn Sie in Frage 18 oben "Ja" geantwortet haben, nennen Sie die Personen ausserhalb des Unternehmens, die Zugang zu den Daten im System haben. Dies könnte Folgendes beinhalten:* • *Kunden* • *Regulierungsbehörde* • *Anbieter für die Bereitstellung von Hosting oder IT-Support* • *Sonstige (Details angeben)*
20.	Welche personenbezogenen Daten werden übermittelt?	*Wenn Sie in Frage 18 oben "Ja" geantwortet haben, könnte die Antwort auf diese Frage lauten:* • *Alle Datenelemente, die in den obigen Fragen 2 und 3 aufgeführt sind, oder* • *Eine Teilmenge der in Frage 2 und 3 aufgeführten Datenelemente [Details angeben].*
21.	Was ist der Zweck der Übertragung?	*Wenn Sie in Frage 18 oben "Ja" geantwortet haben, könnte der Zweck der Übertragung sein:* • *Erbringung von Dienstleistungen für Kunden* • *Erbringung von sonstigen administrativen und IT-Supportleistungen* • *Sonstiges (Details angeben)*

22.	Gibt es einen Vertrag mit dem Dritten? (Bitte legen Sie eine Kopie zur Beurteilung bei.)	*Bitte stellen Sie eine Kopie des Vertrages mit dem Verkäufer zur Verfügung, damit wir prüfen können, ob er angemessene Vertraulichkeits- und Datenschutzbestimmungen enthält, einschliesslich EU-Musterklauseln oder einen Datenübertragungsvertrag.*
	Sicherheitsanforderungen – Datenzugang	
23.	Welche technischen und organisatorischen Sicherheitsmassnahmen muss das System aufweisen, um die personenbezogenen Daten, vertrauliche Daten und sensible personenbezogene Daten vor Verlust, Zerstörung, Beschädigung oder unrechtmässiger Verarbeitung zu schützen?	*Bitte wählen Sie eine der folgenden Optionen:* • *Das System wurde von [Name] IT Security überprüft und entspricht unseren IT-Sicherheitsrichtlinien.* • *Das System wird derzeit überprüft und erst dann eingesetzt, wenn die IT-Security die Einhaltung unserer IT-Sicherheitsrichtlinien bestätigt hat.*
24.	Wer hat Zugang zu den personenbezogenen Daten?	*Geben Sie an, welche Personen, Positionen oder Mitarbeiterkategorien ("Rollen") Zugriff auf welche Elemente oder Datensätze im System haben. Bitte klären Sie ab, ob Personen ausserhalb des Unternehmens Zugang zu den Daten im System haben könnten.*
25.	Welche Zugriffskategorien haben Einzelpersonen, z.B. Nur-Lesen, Bearbeiten, Löschen usw.?	*Erklären Sie für jede der in Frage 24 oben aufgeführten Empfängerrollen:* • *Wo sie sich befinden (Land);* • *Was der Zweck ist, für den Sie Zugang benötigen; und* • *Welche Zugriffsrechte Sie haben (schreibgeschützt, bearbeiten, löschen usw.).* *Bitte stellen Sie uns auch einen Zeitplan mit jeder Rolle und den entsprechenden Zugriffsrechten zur Verfügung, die vom Systemhaus oder unserem IT-Entwickler zur Verfügung gestellt werden sollten.*
26.	Ist es möglich, ein Persönlichkeitsprofil zu generieren, wenn	*Die Antwort auf diese Frage wird wahrscheinlich eine der folgenden sein (bitte wählen Sie eine passende Antwort):*

	eine entsprechende Anfrage vorliegt?	• *Nein.* • *Ja - der Name einer Person kann im System leicht recherchiert / nachgesehen werden, falls die Person einen Antrag auf Zugang zu ihren im System befindlichen Informationen stellt.*
	Datentransfers ausserhalb EWR	
27.	Werden die personenbezogenen Daten ausserhalb des EWR übermittelt?	*Antworten Sie mit "Ja" oder "Nein".* *Bei der Beantwortung dieser Frage ist zu beachten, dass jeder Zugriff auf personenbezogene Daten, der innerhalb des EWR von Parteien ausserhalb des EWR gespeichert wird, eine Übertragung personenbezogener Daten ausserhalb des EWR darstellt.*
28.	Wohin werden die personenbezogenen Daten übermittelt?	*Wenn Sie in Frage 27 oben mit "Ja" geantwortet haben, könnte die Übertragung an einen Standort von Personen erfolgen, die von ausserhalb des EWR auf das System zugreifen.*
29.	Was ist der Zweck der Übertragung, z.B. Speicherung, zusätzliche Zugriffsanforderungen etc.	*Wenn Sie in Frage 27 oben "Ja" geantwortet haben, könnte der Zweck der Übertragung ausserhalb des EWR einer oder mehrere der folgenden sein:* • *Um es Einzelpersonen zu ermöglichen, das System in Übereinstimmung mit dem in Frage 5 dargelegten Zweck zu nutzen* • *Die Erbringung von Dienstleistungen für Kunden.* • *Erbringung von sonstigen administrativen und IT-Supportleistungen* • *Sonstiges (Details angeben)*
30.	Welche Sicherheitsmassnahmen gibt es, um eine sichere Übertragung sowohl personenbezogener Daten als auch sensibler personenbezogener Daten zu gewährleisten?	*Bitte wählen Sie eine der folgenden Optionen:* • *Das System wurde von unserer IT-Security überprüft und entspricht unseren IT-Sicherheitsrichtlinien.* • *Das System wird derzeit überprüft und erst dann eingesetzt, wenn unsere IT-Security die Einhaltung unserer IT-Sicherheitsrichtlinien bestätigt hat.*
31.	Welche Kontrollen gibt es, um eine weitere Übermittlung der personenbezogenen Daten zu verhindern?	*Bitte wählen Sie eine oder beide der folgenden Antworten aus:* • *Die Bedingungen des Dienstleistungsvertrages zwischen uns und dem Systemverkäufer regeln die weitere Übermittlung personenbezogener Daten oder*

		vertraulicher Informationen. Der Zugriff auf diese Informationen ist auf die Mitarbeiter des Lieferanten mit einem definierten Geschäftsbedarf beschränkt. • *Die Verantwortlichen für das System verstehen die Bedeutung der Wahrung des Datenschutzes und der Vertraulichkeit und würden alle Anfragen oder Versuche, Daten in ein anderes System zu übertragen oder anderweitig Informationen aus dem System herunterzuladen, hinterfragen, es sei denn, sie wurden zuvor aus IT- und Datenschutzsicht genehmigt.*

HIAG

Anhang 3 – Verfahrensregeln für den Antrag einer betroffenen Person auf Zugang zu personenbezogenen Daten

Das Datenschutzgesetz gibt dem Einzelnen Rechte, wenn es um den Umgang mit seinen personenbezogenen Daten geht. Diese Rechte können je nach geltender Rechtsprechung variieren (siehe HIAG-Datenschutzerklärung Abschnitt 4.8).

Diese Verfahrensregeln für den Antrag einer betroffenen Person auf Zugang zu personenbezogenen Daten erläutern, wie das Unternehmen mit einem solchen Antrag einer betroffenen Person umgeht (in diesem Verfahren als "**gültiger Antrag**" bezeichnet).

Eine Person, die einen gültigen Antrag an das Unternehmen stellt, hat Anspruch auf die Rechte, die sich aus den geltenden Datenschutzbestimmungen ergeben

1. Antrag

Der Antrag muss schriftlich gestellt werden, wobei auch eine E-Mail ausreichend ist. Unter normalen Umständen wird keine Gebühr erhoben. Dies liegt aber im Ermessen des Unternehmens, sofern dies in Übereinstimmung mit dem anwendbaren Recht ist.

Das Unternehmen muss auf eine gültige Anfrage innerhalb von 30 Kalendertagen (oder einer kürzeren Frist, wie sie im anwendbaren Recht vorgesehen ist) nach Erhalt dieser Anfrage antworten. Das Unternehmen ist nicht verpflichtet, einer Anfrage nachzukommen, falls es keine ausreichenden Informationen erhält, die es dem Unternehmen ermöglichen, die Identität des Antragsstellers zu prüfen.

2. Verfahren

2.1 Erhalt des Antrags

Erhält ein Mitarbeiter oder Unterbeauftragter des Unternehmens eine Anfrage einer Person nach ihren persönlichen Daten, muss dieser die Mitteilung nach Erhalt an die Rechtsabteilung des Unternehmens weiterleiten und dabei das Datum angeben, an dem der Antrag eingegangen ist, zusammen mit allen anderen Informationen, die dem Unternehmen bei der Bearbeitung der Anfrage helfen können.

2.2 Erste Schritte

Das Unternehmen wird eine erste Analyse des Antrags durchführen, um zu entscheiden, ob es sich um einen gültigen Antrag handelt und ob eine Bestätigung der Identität möglich ist oder dazu weitere Informationen erforderlich sind.

Das Unternehmen wird sich dann schriftlich mit dem Antragsteller in Verbindung setzen, um den Erhalt der Anfrage zu bestätigen, dessen Identität zu bestätigen oder, falls erforderlich, weitere Informationen einzuholen oder den Antrag abzulehnen, sofern dies nach geltendem Recht zulässig ist.

2.3 Ausnahmen von Anträgen betroffener Personen

Ein gültiger Antrag kann aus folgenden Gründen abgelehnt werden:

(i) wenn die Weigerung, die Informationen zur Verfügung zu stellen, mit dem geltenden Datenschutzrecht im jeweiligen Land vereinbar ist, oder;

(ii) wenn der Antrag auf Zugang zu den Daten nicht unter die vorstehenden Bestimmungen fällt und:

- wenn es nach Ansicht des Unternehmens notwendig ist, dies zu tun, um die legitimen Geschäftsinteressen des Unternehmens, der nationalen oder öffentlichen Sicherheit, der Verteidigung, der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, zum Schutz der betroffenen Person oder der Rechte und Freiheiten anderer zu schützen; oder
- wenn die personenbezogenen Daten nicht aus einem Land stammen, das den betroffenen Personen das verlangte Recht einräumt, und die Gewährung dieses Rechts vom Unternehmen einen unverhältnismässigen Aufwand erfordert.

2.4 Suche und Antwort

Das Unternehmen veranlasst eine Suche in allen relevanten elektronischen und Papierablagesystemen.

Die angeforderten Informationen werden vom Unternehmen in einem leicht verständlichen Format zusammengestellt (interne Codes oder Identifikationsnummern, die im Unternehmen verwendet werden und den personenbezogenen Daten entsprechen, werden vor der Veröffentlichung übersetzt). Das Unternehmen wird ein Anschreiben erstellen, das die Informationen enthält, die als Antwort auf den Antrag der betroffenen Person auf Zugang zu personenbezogenen Daten erforderlich sind.

Ist die Bereitstellung der Informationen in dauerhafter Form nicht möglich oder mit unverhältnismässigem Aufwand verbunden (sofern nach geltendem Recht zulässig), besteht keine Verpflichtung zur Bereitstellung einer Kopie der Informationen. Die übrigen oben genannten Informationen müssen weiterhin vorgelegt werden. Unter diesen Umständen kann der Person die Möglichkeit geboten werden, durch Einsichtnahme Zugang zu den Informationen zu erhalten oder die Informationen in anderer Form zu erhalten.

2.5 Anträge auf Löschung, Änderung oder Einstellung der Datenverarbeitung

Wenn ein Antrag auf Löschung der personenbezogenen Daten dieser Person eingegangen ist, muss dieser Antrag vom Unternehmen geprüft und gegebenenfalls bearbeitet werden. Wenn eine Anfrage mit dem Hinweis auf eine Änderung der personenbezogenen Daten dieser Person eingeht, müssen diese Informationen korrigiert oder entsprechend aktualisiert werden, wenn das Unternehmen davon ausgeht, dass eine rechtmässige Grundlage dafür besteht.

Wenn die vom Unternehmen vorgenommene Verarbeitung gesetzlich vorgeschrieben ist, gilt der Antrag als nicht gültig.

Alle Fragen im Zusammenhang mit diesem Verfahren sind an den General Counsel zu richten.