Auch wenn aus Gründen der Textautonomie zum Teil auf weibliche Formen verzichtet wurde beziehen sich alle personenbezogenen Formulierungen auf weibliche und männliche Personen.
Bei den Ausführungen handelt es sich nur um eine grobe Orientierungshilfe. Das Dokument kann und soll eine rechtliche Beratung nicht ersetzen. Dementsprechend kann keinerlei Haftung seitens der das Dokument zur Verfügung stellenden Personen oder der Fachgruppe der Wirtschaftskammer Wien für Personenberatung und Personenbetreuung selbst übernommen werden.

DATENSCHUTZ KURZLEITFADEN FÜR DIE ORGANISATION VON PERSONENBETREUUNG (STAND MAI 2018)

Das Datenschutzrecht 2018 bringt neue Dokumentations-, Informations- und Organisationspflichten für Unternehmer mit sich, deren Nichteinhaltung hohe Strafen („wirksam und abschreckend") nach sich ziehen. Für diejenigen, die Datenschutz-Regelungen sorgfältig und individuell in ihrem Unternehmen umsetzen, sieht das Gesetz „Strafmilderung" vor.

„Personenbezogene Daten" sind alle Daten, die jemanden (gegebenenfalls in Kombination mit anderen Daten) als Person identifizieren: Name, Geburtsdatum, Kontostand/Bankdaten, Adresse, Telefonnummer, Orts- und Bewegungsdaten, Fotos, Sozialversicherungsnummer, Kundendaten oder –nummern bei Unternehmen, Ausbildungsnachweise, Zeugnisse, IP-Adressen, Mitgliedsnummer, ...
Besonders schutzwürdige personenbezogene Daten „Sensible Daten" wie etwa Daten zu Gesundheit, Sexueller Orientierung, rassischer und ethnischer Herkunft, Politik, Religion, Gewerkschaftszugehörigkeit, genetische und biometrische Daten müssen noch besser geschützt werden und deren Verarbeitung verlangt unter Umständen eigene Voraussetzungen. Auch „strafrechtlich relevante Daten" genießen einen eigenen Schutz.

Personenbezogene Daten (und zwar nur die, die für den konkreten Zweck erforderlich sind) dürfen im Wesentlichen (in Papierform wie automationsunterstützt) nur verarbeitet werden

- mit gesetzlicher Ermächtigung (Rechnungswesen, Personalverwaltung, ...);
- zur Vertragserfüllung (Erbringung der vertraglich vereinbarten DL);
- mit (u.U. ausdrücklicher) Einwilligung;
- bei Stammkundenbeziehung oder innerhalb Unternehmensgruppe;
- im Notfall (mit Interessenabwägung);
- zur Geltendmachung oder Abwehr von Rechtsansprüchen;
- (weitere Ausnahmen betreffen etwa Gesundheitsvorsorge, Statistische oder Wissenschaftliche Zwecke, Notfallsituationen,...)

Öffentlich bekannte und private personenbezogene Daten sind vom Datenschutzrecht ausgenommen!

Übersicht Ihrer Pflichten:

1. DATENVERFAHRENSVERZEICHNIS

In diesem für JEDES UNTERNEHMEN VERPFLICHTENDen Verzeichnis sind alle Datenverarbeitungen (gleich ob in Papierform oder automationsunterstützt) abzubilden. Die Antwort auf Fragen wie „Wo werden in Ihrem Unternehmen welche Daten für welchen

Zweck verarbeitet?" „An welche Empfänger werden die Daten weitergeleitet?" „Wann werden die Daten gelöscht?" „Wie werden diese Daten geschützt und gesichert?" müssen in Ihrem Verzeichnis zu finden sein.
-> *Gehen Sie das Muster-Verfahrensverzeichnis Anlage ./1 sorgfältig durch, individualisieren Sie es, streichen Sie Unzutreffendes bzw. ergänzen Sie individuelle Anwendungen. Vergessen Sie nicht auf Ihren Webauftritt, Mailverkehr und Ihre mobilen Geräte.*
-> *Halten Sie Ihr Verfahrensverzeichnis immer griffbereit und aktuell (notieren Sie jedes Mal, wenn Sie Ihr Verzeichnis auf Aktualität überprüfen).*

1a. DATENSCHUTZ-FOLGENABSCHÄTZUNG

Die Verpflichtung zur Durchführung (und Dokumentation) einer (rechtlichen und technischen) Datenschutz-Folgenabschätzung ist gegeben, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dies gilt insbesondere bei

- systematischer und umfassender Bewertung persönlicher Aspekte (Profiling, Online-Einstellungsverfahren, Online-Kreditanträge, Videoüberwachung, Gesprächsüberwachung, ...)
- umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten („strafrechtliche relevante Daten" oder „sensible Daten" wie Gesundheitsdaten, zb auch Personalverwaltung)
- systematischer umfangreicher Überwachung öffentlich zugänglicher Bereiche (Videoüberwachung an öffentlichen Plätzen)

-> *wenn Sie im Rahmen Ihrer Personalverwaltung sensible Daten (Religion, Gesundheit/Krankenstand, Gewerkschaftszugehörigkeit ...) dokumentieren (müssen), ODER für Ihre Tätigkeit viele Gesundheitsdaten erheben und übermitteln, ODER einen relevanten Webshop betreiben (Technologie), ODER sonst hochtechnologische/ganz neue/hackeranfällige Software verwenden, ODER Videoüberwachung im Einsatz haben führen Sie bitte (für jeden der genannten Fälle) anhand der Muster in Mappe 2 und 3 der Anlage ./1 eine Datenschutz-Folgenabschätzung durch.*

2. DATENSCHUTZERKLÄRUNG

Diese aus einem individuellen und einem allgemein gültigen Teil bestehende Information hat jeder Unternehmer Personen, deren personenbezogene Daten er speichern will/muss, nachweislich VOR der Aufnahme der Daten zur Kenntnis zu bringen (aushändigen, auf der Webseite zur Verfügung stellen, als Anlage zu einem Mail, ...). Das Dokument informiert, welche Daten Sie zu welchem Zweck verarbeiten, an wen Sie sie gegebenenfalls weiterleiten (müssen) und wann Sie sie löschen (individueller Teil), und enthält eine gesetzliche Belehrung über die Betroffenenrechte (Auskunft, Löschung, Berichtigung, ...).
-> *Passen Sie die Muster-Datenschutzinformation Anlage ./2 anhand Ihres individuellen Datenverfahrensverzeichnisses an. Das Muster stellt auf einen Musterbetrieb OHNE Webanalyse-Tool, Webshop oder Newsletterangebot ab. Sollten Sie derartige Angebote haben müssen Sie die Musterinformation (gegebenenfalls mit externer Hilfe) ergänzen!*
-> *Stellen Sie Ihre Datenschutzinformation allen Personen auf Ihrer Webseite, als Anlage im Mail (später reicht der Hinweis in Ihrer Signatur dass Ihre Datenschutzinformation auf Ihrer*

Webseite unter www.xxx.at zu finden ist) sowie offline in Ihrem Büro/Praxis zur Verfügung, möglichst bevor Sie die Daten dieser Personen verarbeiten.

3. AUFTRAGSVERARBEITERVERTRÄGE

Jeder, der in Ihrem Auftrag die Daten Ihrer Kunden verarbeitet oder Zugriff darauf hat ist „Empfänger der Daten" und „Auftragsverarbeiter" im Sinn des Datenschutzrechtes. Hier fallen beispielsweise Ihr Webhost, Cloud-Anbieter, Mailprovider, ... darunter. Jeder Auftragsverarbeiter ist immer auch Verantwortlicher, nämlich bezüglich Ihrer eigenen Daten als Kunde. Die Frage, ob und inwieweit jemand Auftragsverarbeiter ist, ist schwierig. Jedenfalls aber müssen Sie sich mit jedem der Zugriff auf Daten Ihrer Kunden oder Geschäftspartner hat absichern, dass er das Datenschutzrecht einhält (hier gibt es gegebenenfalls Zertifikate).

-> *Sichern Sie sich bei jedem Empfänger „Ihrer" Daten schriftlich ab (siehe Anlage ./3), dass er/sie datenschutzkonform arbeitet, und vereinbaren Sie konkret, welche Daten er zu welchem Zweck wie lange in Ihrem Auftrag verarbeitet.*

4. EINWILLIGUNGEN

Bei Datenverarbeitungen, für die Ihr Rechtsgrund die „Einwilligung" ist (alle Daten, die Sie nicht aus gesetzlicher Verpflichtung verarbeiten oder für die konkrete Vertragserfüllung benötigen), müssen die Einwilligungen im Bedarfsfall nachgewiesen werden. Die Verarbeitung und/oder Weitergabe sensibler Daten, Fotos, Newsletter- oder Informationsversand, Referenzkundennennung, Werbezusendungen sowie Webauftritt kommen zB in Betracht.

-> *Archivieren Sie alle Einwilligungen, die Sie via Mail, auf Bestell-, Web- oder Anmeldeformularen o.ä. erhalten haben, holen Sie noch vor dem 25.05.2018 ausständige (oder nicht mehr nachweisbare) Einwilligungen ein und beenden Sie alle Tätigkeiten, für die Sie keinen Rechtsgrund (gesetzliche Verpflichtung, Vertragserfüllung, Einwilligung oder klar überwiegende berechtigte Interessen Ihrerseits – Stichwort: Stammkundenpflege) nachweisen können.*

5. UMGANG MIT MITARBEITERN

Mitarbeiter sind in mehrerlei Hinsicht datenschutzrelevant: einerseits müssen Sie Ihre Mitarbeiter nachweislich verpflichten, das Datengeheimnis (personenbezogene Daten aus Ihrem Unternehmen) sowie Geschäfts- und Betriebsgeheimnisse zu wahren (ev. unter Androhung von Konventionalstrafen); andererseits verarbeiten Sie personenbezogene (und sensible Daten) Ihrer Mitarbeiter im Rahmen der Personalverwaltung und müssen diesbezüglich Datenschutzinformationen (siehe oben Punkt 2.) aushändigen; die Erhebung des Religionsverhältnisses, der Gewerkschaftszugehörigkeit, von Notfallkontakten sowie die Verwendung von Fotos, oder das Führen von Geburtstagskalendern sind einwilligungspflichtig (und diese Einwilligungen müssen jederzeit widerrufen werden können); Bewerberunterlagen dürfen für 6 Monate aufbewahrt werden (länger nur mit Einwilligung).

-> *Händigen Sie Ihren Mitarbeitern eigene Datenschutzinformationen gemäß Anlage ./5 aus. Die (gesetzlichen) Aufbewahrungsfristen in Personalsachen liegen teilweise bei 30 Jahren – weisen Sie darauf hin.*

-> *Schließen Sie mit Ihren Mitarbeitern eine Verpflichtungserklärung zur Einhaltung des Datengeheimnisses und der Wahrung Ihrer Geschäfts- und Betriebsgeheimnisse gemäß Anlage ./6 ab und archivieren Sie diese Erklärungen in den Personalakten.*
-> *Holen Sie von Ihren Mitarbeitern Einwilligungen zur allfälligen Verarbeitung des Religionsverhältnisses, der Gewerkschaftszugehörigkeit, von Notfallskontakten und/oder Fotos ein und archivieren Sie diese.*

DATENSICHERHEITSMASSNAHMEN

Das Datenschutzrecht verlangt, dass Sie die Vertraulichkeit, Integrität und Verfügbarkeit aller personenbezogenen Daten in Ihrem Unternehmen zu jedem Zeitpunkt gewährleisten. Als Sicherungsmaßnahmen kommen zB in Betracht: Schlüssel, Code, Passwort, Safe, Automatische Sperrmechanismen, Alarmanlage, Zugriffsbeschränkung, Eingabekontrolle, Verschlüsselung von Endgeräten, Ordnern und Datenübermittlungen, Pseudonymisierung, Back-Ups, Firewalls, ...
-> *Überprüfen Sie bei allen Datenverarbeitungen einzeln, ob Sie sämtliche zumutbaren organisatorischen und IT-Sicherungsmaßnahmen ergriffen haben, und ob diese in Ihrem Verfahrensverzeichnis abgebildet sind. Bei Papierform ist es immer zumutbar, zu anonymisieren, und die Unterlagen ausschließlich versperrt aufzubewahren.*

DATA-BREACH-PROZESSE

Jeder Verlust, jede Veränderung, jede Vernichtung und jede unbefugte Offenlegung personenbezogener Daten ist eine Datenschutzverletzung im Sinn der DSGVO und ist der Datenschutzbehörde binnen 72 Stunden zu melden. Das kann der Verlust eines USB-Sticks, der Diebstahl Ihres Mobiltelefones (wenn da Kontakte von Kunden/Geschäftspartnern drauf sind), ein Hackerangriff oder auch ein Brand in Ihren Büroräumlichkeiten sein. (Unter Umständen müssen Sie sogar alle betroffenen Personen, deren Daten verloren, verändert, vernichtet oder offengelegt wurden informieren).
-> *Schaffen Sie nachweislich Prozesse in Ihrem Unternehmen, damit Ihnen Datenschutzverletzungen zeitnah gemeldet werden und Sie innerhalb der Frist eine Meldung machen können.*

HINWEIS: Sowohl aktuelle, als auch „alte" Kunden- und Geschäftsbeziehungen bzw. Datenverarbeitungen müssen ab dem 25.05.2018 datenschutzkonform sein. Setzen Sie daher alle erforderlichen Maßnahmen Schritt für Schritt in Ihrem Unternehmen um.

Urheber: Dr. Geraldine Treitler, Stand Mai 2018