Greiter
Pegger
Kofler

Rechtsanwälte

Datenschutzrecht

Überblick und Umsetzung

(mit Checkliste)

RA Dr. Georg Huber, LL.M. (Univ. of Chicago)

Zertifizierter Datenschutzbeauftragter

Akadem. gepr. Europarechtsexperte

Stand: September 2018

Inhalt

Impressum
Medieninhaber und Herausgeber:
Greiter Pegger Kofler & Partner Rechtsanwälte

Maria-Theresien-Straße 24
6020 Innsbruck, Austria
Telefon: +43 512 57 18 11
Fax: +43 512 58 49 25
office@lawfirm.at
www.lawfirm.at

Datenschutzrecht

Überblick und Umsetzung (mit Checkliste)

RA Dr. Georg Huber, LL.M. (Univ. of Chicago)

Zertifizierter Datenschutzbeauftragter
Akadem. gepr. Europarechtsexperte

Über den Autor
Rechtsanwalt Dr. Georg Huber, LL.M. (Chicago) ist Partner in der Kanzlei Greiter Pegger Kofler & Partner. Er befasst sich insbesondere mit IT/IP-Recht, einschließlich des Datenschutzrechtes, sowie Gesellschafts-, Kartell- und Vertriebsrecht. Er ist zertifizierter Datenschutzbeauftragter (TÜV Österreich) und akademisch geprüfter Europarechtsexperte.

Greiter Pegger Kofler | Rechtsanwälte

1 Einleitung

Am 25. Mai 2018 trat die EU-Datenschutz-Grundverordnung (DSGVO) in Kraft, die erstmals für ein in weiten Teilen einheitliches Datenschutzrecht in der gesamten EU sorgen wird. Mit gleichem Datum wurde auch das österreichische Datenschutzgesetz (DSG) umfassend angepasst.

Die DSGVO ändert im Wesentlichen nichts an der grundsätzlichen Zulässigkeit einer Datenverarbeitung. Sie verlangt aber insbesondere, dass Datenverarbeitungen genau dokumentiert werden und sowohl gegenüber der Datenschutzbehörde als auch gegenüber den einzelnen Betroffenen die Einhaltung der Bestimmungen der DSGVO nachgewiesen werden kann (Rechenschaftspflicht). Dies erfordert einigen Aufwand.

Mit der DSGVO hat auch insofern ein Paradigmenwechsel stattgefunden, als die Verantwortung für den Datenschutz ausschließlich in die Hände der Unternehmen gelegt wird. Die Datenschutzbehörden genehmigen nicht mehr vorab die Datenverarbeitungen, sondern prüfen und strafen allenfalls im Nachhinein.

Im Folgenden erhält der Leser einen Überblick über das Datenschutzrecht und anschließend eine kurze Handlungsanleitung (samt Checkliste) für die Umsetzung im Unternehmen. Beides kann eine ausführliche, auf den jeweiligen Einzelfall abgestimmte Beratung, nicht ersetzen, sondern dient nur einer ersten Orientierung.

2 Überblick Datenschutzrecht

2.1 Grundsätze des Datenschutzes

Datenschutz hat nicht das Ziel, „Daten“ zu schützen, sondern Personen. Jede natürliche Person hat ein Grundrecht darauf, dass ihre Privatsphäre geachtet und gewahrt wird. Dazu zählt auch, dass jeder selbst über die Preisgabe und Verwendung seiner Daten bestimmen kann („informationelle Selbstbestimmung“) und dass seine Daten geheim gehalten werden.

Dieser übergeordneten Zielsetzung folgend ist das Datenschutzrecht von einigen Grundsätzen geprägt, an denen sich die Rechte und Pflichten der Datenverarbeiter und der betroffenen Personen orientieren.

Im Einzelnen sind dies folgende Grundsätze:

- Verarbeitung nach Treu und Glauben:
  Datenverarbeitungen müssen redlich erfolgen.
- Rechtmäßigkeit:
  Datenverarbeitungen sind verboten, es sei denn, das Gesetz erlaubt sie. Siehe dazu Punkt 2.4.
- Transparenz:
  Betroffene müssen wissen, wer welche ihrer Daten wofür verarbeitet. Siehe dazu Punkt 2.8.
- Richtigkeit:
  Die verarbeiteten Daten müssen korrekt sein.
- Zweckgebundenheit:
  Der Zweck jeder Datenverarbeitung muss im Vorhinein konkret bestimmt sein und es darf keine mit diesem Zweck inkompatible Nutzung der Daten erfolgen.
- Datenminimierung:
  Datenverarbeitungen sollen auf das erforderliche Maß begrenzt werden (Datensparsamkeit).
- Integrität und Vertraulichkeit:
  Daten müssen vor Manipulation und dem Bruch des Datengeheimnisses geschützt werden.

Der „Verantwortliche“ der Datenverarbeitung muss für die Einhaltung dieser Grundsätze

sorgen. Er ist dafür rechenschaftspflichtig und muss ihre Einhaltung nachweisen können.

2.2 Einige Grundbegriffe

2.2.1 Personenbezogene Daten

Personenbezogene Daten sind alle Informationen über eine identifizierte oder identifizierbare natürliche Person. Das sind zB Name, Adresse, Sozialversicherungsnummer, Email-Adresse aber auch die IP-Adresse des Computers einer Person und Fotos/Videos. Der Begriff ist weit gefasst.

2.2.2 Dateisystem

Ein Dateisystem ist jede strukturierte Datensammlung, die nach bestimmten Kriterien zugänglich ist. Es ist unerheblich, ob sie manuell (zB Karteikarten) oder automatisationsunterstützt geführt wird. Alle Dateisysteme unterliegen der DSGVO.

2.2.3 Verarbeitung

Das ist jeder manuelle oder automatisierte Vorgang im Zusammenhang mit personenbezogenen Daten, wie zB das Erheben, Erfassen, Berichtigen, Speichern, Löschen, Ordnen, Übermitteln, Offenlegen, Auslesen oder Verbreiten.

2.2.4 Verantwortlicher

Der „Verantwortliche“ ist jene natürliche oder juristische Person oder Behörde, die über Mittel und Zweck der Datenverarbeitung entscheidet. In der Regel ist die Geschäftsleitung oder der Unternehmensinhaber der Verantwortliche.

2.2.5 Auftragsverarbeiter

Ein „Auftragsverarbeiter“ ist jene natürliche oder juristische Person oder Behörde, die im Auftrag und über Weisung des Verantwortlichen personenbezogene Daten verarbeitet.

Das sind beispielsweise Druckereien (die ein Mailing drucken), ein Call Center, das eine Telefonaktion durchführt oder Dialog Marketing-Agenturen, die Daten für eine Marketingkampagne aufbereiten.

Manchmal ist die Abgrenzung hin zum Verantwortlichen schwierig.

2.2.6 Betroffener

Ein „Betroffener“ ist jene natürliche Person, deren Daten verarbeitet werden.

2.2.7 Besondere Datenkategorien

Zu den besonderen Datenkategorien („sensible Daten“) zählen:

- Strafrechtliche Verurteilungen,
- Gesundheitsdaten,
- Genetische und biometrische Daten,
- Daten zum Sexualleben,
- Daten zur rassischen oder ethnischen Herkunft,
- Daten zur politischen, weltanschaulichen und religiösen Überzeugung,
- genetische und biometrische Daten (zB Fingerabdruck),
- Gewerkschaftszugehörigkeit.

Wirtschaftliche Daten, wie zB das Einkommen, zählen nicht zu den besonderen Datenkategorien.

2.3 Wer hat den Datenschutz zu beachten?

Der Datenschutz ist von jedem zu beachten, mit wenigen Ausnahmen. Ausgenommen sind insbesondere natürliche Personen, wenn sie persönliche oder familiäre Datenverarbeitungen betreiben.

Daher sind alle Unternehmen, Vereine und sonstigen Organisationen gehalten, den Datenschutz zu beachten. Für die Strafverfolgungsbehörden gelten eigene Bestimmungen.

Voraussetzung ist, dass Datenverarbeiter entweder (i) in der EU eine Niederlassung haben, (ii) dort geschäftlich tätig sind oder (iii) das

Verhalten von Personen in der EU beobachten („Marktortprinzip“).

Somit können auch Unternehmen außerhalb der EU von der DSGVO betroffen sein. Wenn solche Unternehmen keine Niederlassung in der EU haben, müssen sie in der EU einen „Vertreter“ bestellen.

2.4 Wann ist eine Datenverarbeitung erlaubt?

2.4.1 Allgemeines

Die Verarbeitung personenbezogener Daten ist verboten, es sei denn, sie erfolgt „rechtmäßig“. Rechtmäßig erfolgt sie dann, wenn die DSGVO die Verarbeitung erlaubt.

Für jede einzelne Datenverarbeitung muss es daher eine Rechtfertigung geben (= Rechtmäßigkeit der Verarbeitung, siehe dazu Punkt 2.4.2), wobei zwischen „normalen“ (nicht sensiblen) personenbezogenen Daten und den „besonderen Datenkategorien“ unterschieden werden muss.

2.4.2 Rechtmäßigkeit

Folgende Rechtsgrundlagen kommen dafür in Frage (gilt nicht für die besonderen Datenkategorien – siehe dazu Punkt 2.4.3):

- Erfüllung eines Vertrags:

  zB das Unternehmen muss die Daten seiner Kunden und Lieferanten zum Zweck der Geschäftsabwicklungen verarbeiten.
- Erfüllung einer rechtlichen Verpflichtung:

  zB Mitarbeiterdaten müssen aufgrund arbeits- und sozialversicherungsrechtlicher Vorschriften verarbeitet werden.
- Schutz lebenswichtiger Interessen des Betroffenen:

  zB ein vermisster Bergsteiger wird über sein Mobiltelefon geortet, um ihn zu retten.
- Erfüllung einer Aufgabe im öffentlichen Interesse:

  zB wissenschaftliche Forschung im Bereich der Medizin.
- Überwiegendes Interesse des Verantwortlichen oder eines Dritten gegenüber den Interessen des Betroffenen:

  zB Datenverarbeitung für Zwecke der Direktwerbung (Achtung: Hier ist eine Interessensabwägung vorzunehmen).
- Einwilligung des Betroffenen (siehe hiezu Punkt 2.6).

2.4.3 Besondere Datenkategorien

Zur Frage, welche Daten unter die „besonderen Datenkategorien“ fallen, siehe Punkt 2.2.7.

Für die besonderen Datenkategorien gelten die vorhin in Punkt 2.4.2 dargestellten Rechtmäßigkeitsgründe nicht. Insbesondere dürfen bei ihnen die Datenverarbeitungen nicht auf den Rechtmäßigkeitsgrund der „Vertragserfüllung“ oder die „überwiegenden berechtigten Interessen“ gestützt werden.

In der Regel ist die Verarbeitung besonderer Datenkategorien nur dann möglich, wenn

- eine ausdrückliche Einwilligung vorliegt,
- die Verarbeitung erforderlich ist, um arbeits- und sozialrechtliche Verpflichtungen zu erfüllen,
- Rechtsansprüche geltend gemacht oder abgewehrt werden sollen, oder
- die Verarbeitung aus gesundheitspolitischen Gründen erforderlich ist (zB Gesundheitsvorsorge, Arbeitsmedizin).

Die genaue Auflistung der Rechtmäßigkeitsgründe findet sich in Art. 9 Abs. 2 DSGVO. Für die Verarbeitung strafrechtlicher Verurteilungen ergibt sich die Rechtmäßigkeit aus nationalem Recht.

2.5 Bei welchen Datenverarbeitungen ist besondere Vorsicht geboten?

2.5.1 Allgemeines

Allgemein sollte man besonders dann vorsichtig sein, wenn besondere Datenkategorien (siehe Punkt 2.2.7) verarbeitet werden, oder wenn für die Betroffenen ein hohes Risiko besteht.

Oft wird beides zusammenhängen, aber es gibt auch hohe Risiken außerhalb der besonderen Datenkategorien. Ein Arzt verarbeitet zB viele Gesundheitsdaten. Gelangen diese Daten an die Öffentlichkeit, besteht in der Regel ein hohes Risiko für die Betroffenen. Sie sind erheblich in ihrem Grundrecht auf Privatheit verletzt.

Ein hohes Risiko kann aber etwa auch dann vorliegen, wenn Passwörter oder Kreditkartendaten gestohlen werden.

2.5.2 Besondere Datenkategorien

Bei diesen Daten ist ein besonderes Augenmerk auf die Rechtmäßigkeit der Datenverarbeitung zu legen (siehe Punkt 2.4.2).

Abgesehen davon sind diese Daten besonders zu schützen (siehe Punkt 2.10).

2.5.3 Drittlandübermittlungen

Bei der Übermittlung von personenbezogenen Daten ins EU-Ausland muss immer geprüft werden, ob die Übermittlung zulässig ist.

Eine Voraussetzung dafür ist, dass die Daten rechtmäßig verarbeitet werden.

Daneben müssen aber noch weitere Voraussetzungen erfüllt sein, die bei besonderen Datenkategorien wiederum enger gefasst sind. Siehe hiezu Punkt 2.12.

2.6 Wann braucht man eine Einwilligung und wie muss diese aussehen?

2.6.1 Allgemeines

Eine Einwilligung ist nur dann erforderlich, wenn kein anderer Rechtsmäßigkeitsgrund greift (vgl Punkt 2.4).

Bei vielen Datenverarbeitungen wird daher eine Einwilligung gar nicht erforderlich sein. Sie dürfen bereits aus einem anderen Grund rechtmäßig durchgeführt werden, zB weil die Datenverarbeitung zur Abwicklung eines Vertrages erforderlich ist.

Das zusätzliche Einholen von Einwilligungen „zur Sicherheit“ sollte eher vermieden werden, weil Einwilligungen jederzeit widerrufen werden können und ein Widerruf der Einstellung möglicherweise auch gleichzeitig als Widerspruch (siehe Punkt 2.13.8) gegen eine an sich gerechtfertigte Verarbeitung gewertet werden könnte.

2.6.2 Formale Voraussetzungen für eine Einwilligung

Damit eine Einwilligung wirksam ist und bestehende Einwilligungen wirksam bleiben (letztere sind daher zu überprüfen), müssen folgende Voraussetzungen vorliegen:

- Ausreichende Information, wozu eingewilligt werden soll (Zweck, betroffene Datenkategorien, allfällige Datenempfänger, maximale Speicherdauer);
- Information über die Möglichkeit des jederzeitigen Widerrufs;
- Verständliche Formulierung;
- Freiwilligkeit, kein faktischer Zwang zur Einwilligung:

  Freiwilligkeit liegt zB dann nicht vor, wenn der Kunde ein Produkt nur dann kaufen kann, wenn er vorher seine Einwilligung zum Erhalt des monatlichen Newsletters erteilt hat. Damit wird er faktisch zur Einwilligung gezwungen, sodass sie mangels Freiwilligkeit nicht wirksam ist („Koppelungsverbot“);
- Gesonderte Einwilligung für jede einzelne Datenverarbeitung (keine „Sammeleinwilligung“);

> Vorgefertigte Einwilligungserklärungen sollten von einem Experten geprüft werden.

Minderjährige können erst ab Vollendung des 14. Lebensjahres wirksam einwilligen, jedenfalls soweit Dienste der Informationsgesellschaft betroffen sind. Sonst ist die Einwilligung des gesetzlichen Vertreters erforderlich.

Eine Einwilligung kann schriftlich, mündlich oder auch schlüssig (zB durch Kopfnicken) erfolgen. Aus Beweisgründen empfiehlt es sich jedoch – sofern möglich – eine schriftliche Einwilligung (zB durch Setzen eines Häkchens neben der Datenschutzerklärung bei einer Online-Bestellung oder durch Abdrucken der Datenschutzerklärung auf der Rückseite eines Anmeldeformulars samt gesondertem Unterschriftsfeld einzuholen).

Für besondere Datenkategorien ist eine „ausdrückliche" Einwilligung erforderlich. Für manche Drittlandübermittlungen bedarf es einer „informierten Einwilligung", dh der Einwilligende muss über die datenschutzrechtlichen Risiken der Drittlandübermittlung aufgeklärt werden.

2.7 Wer braucht einen Datenschutzbeauftragten und was macht er?

Die Bestellung eines Datenschutzbeauftragten ist nur dann erforderlich, wenn die „Kerntätigkeit" des Unternehmens entweder (i) in der umfangreichen Verarbeitung besonderer Datenkategorien oder (ii) in der regelmäßigen, systematischen und umfangreichen Überwachung von Personen besteht.

Behörden und öffentliche Stellen (zB Körperschaften öffentlichen Rechts) müssen immer einen Datenschutzbeauftragten bestellen.

Idealerweise bringt diese Person sowohl juristisches als auch technisches Verständnis mit und kennt die Abläufe im Unternehmen. Sie muss zumindest über ein bestimmtes Fachwissen verfügen, wenn es auch keine formellen Qualifikationserfordernisse gibt.

Der Datenschutzbeauftragte kann entweder ein Mitarbeiter oder ein externer Berater sein.

Die Aufgaben des Datenschutzbeauftragten umfassen Folgendes:

> Er berät Unternehmen und Mitarbeiter zum Datenschutz. Er ist jedoch nicht für die Umsetzung verantwortlich.

> Er überwacht die Umsetzung des Datenschutzes.

> Er berät im Zusammenhang mit einer Datenschutz-Folgenabschätzung.

> Er ist die Anlauf- und Kontaktstelle für die Datenschutzbehörde.

Der Datenschutzbeauftragte berichtet zwingend der obersten Geschäftsführungsebene. Ein Mitglied der Geschäftsführung kann nicht zum Datenschutzbeauftragten bestellt werden, da hier ein Interessenskonflikt bestünde.

Der Datenschutzbeauftragte agiert im Bereich des Datenschutzes unabhängig und weisungsfrei. Er unterliegt in dieser Funktion auch einem Kündigungsschutz (sofern er ein Mitarbeiter ist).

2.8 Information der Betroffenen

2.8.1 Allgemeines

Transparenz ist einer der Grundsätze des Datenschutzes. Das bedeutet, dass jeder Betroffene zumindest die Möglichkeit haben muss, zu erfahren, wer welche seiner Daten zu welchem Zweck verarbeitet.

Diese Information muss vom Verantwortlichen proaktiv bei Erhebung der Daten bereitgestellt werden. Die Information ist in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Es ist zulässig, Bildsymbole zu verwenden.

Der exakte Inhalt der Information ergibt sich aus den Art. 13 und 14 DSGVO, wobei zu

unterscheiden ist, ob der Verantwortliche die Information vom jeweils Betroffenen selbst oder von einem Dritten erhält.

2.8.2 Daten kommen direkt vom Betroffenen

Art. 13 DSGVO zählt alle Informationen auf, die dem Betroffenen erteilt werden müssen, wenn die Daten direkt bei ihm erhoben werden. Im Wesentlichen sind dies folgende Informationen:

- Namen und die Kontaktdaten des Verantwortlichen.
- Kontaktdaten des Datenschutzbeauftragten.
- Zweck und Rechtsgrundlage der Verarbeitung; sofern sich der Verantwortliche auf seine berechtigten Interessen stützt, sind diese zu nennen.
- Empfänger der personenbezogenen Daten.
- Information zu Drittlandübermittlungen.
- Dauer der Speicherung oder die Kriterien für die Festlegung dieser Dauer;
- Information über die Betroffenenrechte (vgl Punkt 2.13).
- Information über das jederzeitige Widerrufsrecht bei Einwilligungen.
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde.
- Ob eine Verpflichtung zur Bereitstellung der Daten besteht oder ob diese für den Vertragsabschluss erforderlich sind.
- Ob eine automatisierte Entscheidungsfindung einschließlich Profiling besteht und Informationen über die involvierte Logik und Tragweite für die betroffene Person.

2.8.3 Daten stammen von einem Dritten

Art. 14 DSGVO bestimmt, welche Informationen zu erteilen sind, wenn die Daten nicht direkt bei der betroffenen Person erhoben werden.

Dies ist neben den in Art. 13 DSGVO genannten Informationen im Wesentlichen die Quelle aus der die personenbezogenen Daten stammen.

Die Informationen sind in einer angemessenen Frist ab Erlangung der Daten, längstens binnen eines Monats oder im Zuge der ersten Kommunikation oder bei Offenlegung an einen Dritten, bereitzustellen.

2.8.4 Wie kann die Information bereitgestellt werden?

Es gibt verschiedene Möglichkeiten, wie die erforderlichen Informationen bereitgestellt werden können. Es ist aber in jedem Einzelfall zu prüfen, ob die gewählte Art und Weise ausreichend ist. Folgende Methoden können grundsätzlich ausreichend sein:

- Datenschutzerklärung auf der Website (dann, wenn die betroffene Person leichten Zugang zum Internet hat).
- Papierform, zB in Arbeitsverträgen, Aushängen, auf Formularen etc.
- Telefonisch (zB bei Meinungsumfragen): mündliche Information durch eine natürliche Person oder auch automatisierte Information (zB auf Tonband), allenfalls mit der Möglichkeit zusätzlich Fragen zu stellen.
- Geräte ohne Display (Internet der Dinge): Es könnten zB QR-Codes, Bildsymbole, schriftliche Information in Papierform (zB in der Bedienungsanleitung) verwendet werden.
- Videoüberwachung: Schilder, die die Informationen beinhalten.

Besonderes Augenmerk sollte man auch auf die Sprache legen. Der Betroffene muss in der Lage sein, die Information zu verstehen. Kommuniziert man daher zB mit einem Betroffenen auf Englisch, wird auch die Information in dieser Sprache bereitgestellt werden müssen.

2.9 Welche Dokumentation muss ich erstellen?

2.9.1 Verarbeitungsverzeichnis

Das „Verzeichnis von Verarbeitungstätigkeiten“ ersetzt die bisherige Meldung an das Datenverarbeitungsregister.

Es enthält alle Datenverarbeitungen im Unternehmen und beschreibt die technischen und organisatorischen Maßnahmen, die das Unternehmen zur Gewährleistung eines angemessenen Sicherheitsniveaus ergriffen hat.

Die Datenverarbeitungen sind unter Angabe von Zweck, Datenkategorien, Empfänger, Löschfrist, Rechtsgrundlage etc. aufzulisten. Fast jedes Unternehmen muss es zwingend erstellen. Das kann auch in Form einer Excel-Tabelle erfolgen.

Ein Muster bietet die Wirtschaftskammer Österreich (www.wko.at/datenschutz) an.

2.9.2 Auftragsverarbeiterverträge

Auftragsverarbeiter sind Unternehmen oder natürliche Personen, die im Auftrag eines Verantwortlichen Daten verarbeiten (vgl Punkt 2.2.5). Sie dürfen nur auf schriftliche Weisung des Verantwortlichen tätig sein.

Mit Auftragsverarbeitern muss ein Vertrag nach Art. 28 DSGVO abgeschlossen werden. Es dürfen nur solche Auftragsverarbeiter beauftragt werden, die bestätigen oder nachweisen können, dass sie die Vorgaben der DSGVO einhalten.

Auftragsverarbeiter haften für Verstöße gegen die DSGVO, die in ihrer Einflusssphäre stattfinden. Verantwortliche haften solidarisch gegenüber den Betroffenen für solche Verstöße.

Ein Muster bietet die Wirtschaftskammer Österreich (www.wko.at/datenschutz) an.

2.9.3 Datenschutzerklärung

Auf jeder Homepage muss eine Datenschutzerklärung zu finden sein.

Sie dient dazu, den Besucher der Homepage über Datenverarbeitungen zu informieren. Vergleiche dazu Punkt 2.8.

2.9.4 Einwilligungen

Soweit Einwilligungen überhaupt benötigt werden, sind sie sorgfältig zu erstellen und entsprechend zu dokumentieren. Siehe dazu Punkt 2.6.

Das Vorhandensein von Einwilligungen muss vom Verantwortlichen jederzeit nachgewiesen werden können.

Gleichermaßen sollte sichergestellt werden, dass Datenverarbeitungen beendet werden, wenn Einwilligungen widerrufen werden. Auch hier empfiehlt sich eine entsprechende Dokumentation.

2.9.5 Verpflichtung der Mitarbeiter zum Datengeheimnis

Jeder Verantwortliche muss seine Mitarbeiter zur Wahrung des Datengeheimnisses (auch nach Beendigung des Dienstverhältnisses) verpflichten. Eine Ausnahme von dieser Verpflichtung besteht nur dann, wenn die Mitarbeiter bereits von Gesetzes wegen zur Verschwiegenheit verpflichtet sind.

Es empfiehlt sich daher, entweder den Arbeitsvertrag um einen entsprechenden Passus zu ergänzen oder die Mitarbeiter eigene Verpflichtungserklärungen unterfertigen zu lassen. Ein Muster bietet die Wirtschaftskammer Österreich (www.wko.at/datenschutz) an.

2.9.6 Vertrag für „gemeinsam Verantwortliche“

Wenn zwei oder mehrere Personen den Zweck und die Mittel der Verarbeitung personenbezogener Daten festlegen, sind sie „gemeinsam Verantwortliche“.

Ein Anwendungsfall ist etwa die gemeinsame Errichtung einer Infrastruktur, auf der mehrere Beteiligte ihre jeweils individuellen Zwecke

verfolgen, zB gemeinsames Betreiben einer internetgestützten Plattform für Reisereservierungen durch ein Reisebüro, eine Hotelkette und eine Fluggesellschaft oder eine gemeinsame Plattform zum Betrieb eines regionalen Skipools.

Auch Betreiber einer Fanpage auf Facebook dürften nach einem Urteil des EuGH (C-210/16) zusammen mit Facebook als „gemeinsam Verantwortliche" gelten (siehe dazu Punkt 3.3.10).

Gemeinsam Verantwortliche haben einen Vertrag nach Art. 26 DSGVO abzuschließen, in dem geregelt wird, welchem Verantwortlichen welche Verpflichtung nach der DSGVO zukommen. Insbesondere ist zu regeln, wer die Betroffenenrechte wahrnimmt (siehe dazu Punkt 2.13).

Der wesentliche Inhalt dieser Vereinbarung ist den betroffenen Personen offen zu legen.

2.9.7 Datenschutz-Folgenabschätzung

Wenn aufgrund einer Datenverarbeitung ein hohes Risiko für die Betroffenen besteht, ist vorab eine Datenschutz-Folgenabschätzung durchzuführen. Dabei handelt es sich um eine vertiefte Risikoanalyse. Daraus sind dann Abhilfemaßnahmen abzuleiten.

Wenn die Maßnahmen zu keiner Verringerung des Risikos führen, ist die Datenschutzbehörde zu konsultieren.

Die Datenschutz-Folgenabschätzung ist insbesondere dann erforderlich, wenn neue Technologien eingesetzt werden (zB seinerzeit die „Smart Meter"), beim systematischem, umfassenden Profiling mit anschließender automatisierter Entscheidungsfindung, bei der umfangreichen Bearbeitung sensibler Daten oder von Strafrechtsdaten und bei der systematischen Überwachung öffentlich zugänglicher Bereiche.

Die Datenschutzbehörden müssen Black-/White-Lists erlassen, aus denen hervorgeht, wann jedenfalls eine Datenschutz-Folgenabschätzung gemacht werden muss und wann nicht. Die entsprechende White-List Verordnung der österreichischen Datenschutzbehörde wurde im Bundesgesetzblatt (BGBl. II Nr. 108/2018) veröffentlicht.

2.9.8 Sonstiges

Wesentlich ist, dass eine umfassende und ordentliche Dokumentation angefertigt wird, und zwar sowohl elektronisch als auch auf Papier.

Darin sollten alle Überlegungen festgehalten sein, zB warum gegebenenfalls kein Datenschutzbeauftragter bestellt wird, warum keine Datenschutz-Folgenabschätzung erfolgt, welche TOMs (siehe Punkt 2.10) ergriffen wurden, wann und wie oft die Mitarbeiter geschult wurden, etc.

Diese Dokumentation soll in erster Linie dem Verantwortlichen dazu dienen, über die Einhaltung der Pflichten nach der DSGVO Rechenschaft ablegen zu können. Dazu ist er verpflichtet (siehe Punkt 2.1).

2.10 Was gilt in puncto Datensicherheit?

Personenbezogene Daten sind zu schützen. Das heißt, jeder Verantwortliche und jeder Auftragsverarbeiter muss ein „angemessenes Schutzniveau" gewährleisten, damit die Integrität, Vertraulichkeit und Verfügbarkeit der Daten sowie die Belastbarkeit seiner Systeme gesichert ist.

Das „angemessene Schutzniveau" bestimmt sich anhand verschiedener Kriterien. Dabei ist vom jeweiligen Stand der Technik auszugehen, aber auch von den Implementierungskosten, der Art und dem Umfang der Daten und des Risikos, das für Betroffene bei einer Verletzung des Datenschutzes besteht. Es macht daher einen Unterschied, ob ein kleiner Verein nur ohnehin allgemein zugängliche Mitgliederdaten (z.B. Name und Adresse) oder ein Krankenhaus umfangreiche Gesundheitsdaten verarbeitet.

Jeder Verantwortliche und jeder Auftragsverarbeiter muss geeignete technische und organisatorische Maßnahmen (TOMs) vorsehen und muss diese auch dokumentieren. Dazu zählen etwa Firewalls, Virenschutz, aktuelle Software-Updates, Backups, Pseudonymisierung von Daten, Verschlüsselungen, Schulungen für Mitarbeiter, Erlassung interne Datenschutzrichtlinien, „clean desk policy", Zugriffsberechtigungen, Zugriffsbeschränkungen, uä.

Diese TOMs müssen so ausgelegt sein, dass die Datenschutzgrundsätze wirksam umgesetzt und der DSGVO Rechnung getragen wird.

2.11 Wie gehe ich mit Mitarbeiterdaten um?

Die personenbezogenen Daten der Mitarbeiter dürfen in der Regel ohne Einwilligung verarbeitet werden, insbesondere dort, wo eine rechtliche Verpflichtung nach arbeits- und abgabenrechtlichen Vorschriften besteht.

Sensible Daten der Mitarbeiter, zB Religionsbekenntnis oder Gewerkschaftszugehörigkeit, dürfen ebenfalls ohne Einwilligung im Rahmen der arbeits- und sozialrechtlichen Vorschriften verarbeitet werden (Art. 9 Abs. 2 lit b DSGVO).

Kritisch ist hingegen die Verarbeitung von Mitarbeiterfotos, zB für die unternehmenseigene Homepage oder in der Email-Signatur. Hier wird in der Regel eine Einwilligung erforderlich sein (siehe dazu Punkt 2.14). Bei der Einholung von Einwilligungen von Mitarbeitern ist besonders darauf Bedacht zu legen, dass diese freiwillig erfolgen.

Im Rahmen der Sicherheit muss darauf geachtet werden, dass innerhalb des Unternehmens nur jene Personen Zugang zu Mitarbeiterdaten haben, die diese auch tatsächlich benötigen. Das sind üblicherweise die Personalabteilung, die Geschäftsleitung und allenfalls auch die Abteilungsleiter für die ihnen direkt unterstellten Mitarbeiter.

Bei der Löschung von Mitarbeiterdaten gelten die Ausführungen unter Punkt 2.17. Daten von Bewerbern, die nicht angestellt werden, sind normalerweise binnen sechs Monaten zuzüglich einer kurzen Pufferfrist zu löschen.

Nähere Informationen zum Thema Arbeitnehmerdatenschutz finden Sie in unserer Broschüre „HR-Daten: Gebotenes, Erlaubtes und Verbotenes" von unserem Kanzleipartner RA Dr. Herwig Frei.

2.12 An wen darf ich Daten weitergeben?

Daten dürfen nur dann weitergegeben werden, wenn sie rechtmäßig verarbeitet werden (siehe Punkt 2.4). Auch die Weitergabe darf nur erfolgen, wenn sie rechtmäßig und zweckentsprechend ist (zum „Zweckbindungsgrundsatz" siehe Punkt 2.1).

Besondere Vorsicht ist bei Drittlandübermittlungen geboten. Bei solchen Übermittlungen verlieren die personenbezogenen Daten den Schutz nach der DSGVO, weil diese in Drittländern nicht gilt.

Daher sind solche Übermittlungen nur unter bestimmten Voraussetzungen zulässig. Im Wesentlichen sind dies Folgende:

- Die EU-Kommission hat mit Beschluss festgestellt, dass im betreffenden Land ein angemessenes Datenschutzniveau herrscht („Angemessenheitsbeschluss"). Das ist etwa bei der Schweiz, Kanada, Argentinien, Neuseeland und den USA (dort aber nur nach Maßgabe des „Privacy Shield") erfolgt.
- Abschluss sogenannter Standarddatenschutzklauseln zwischen dem Übermittler und dem Empfänger im Drittstaat.
- Innerhalb eines Konzernes bei behördlich genehmigten „Binding Corporate Rules" (BCR).
- Informierte Einwilligung des Betroffenen.

- Abschluss oder Erfüllung eines Vertrages mit dem Betroffenen oder in seinem Interesse.
- Übermittlung zur Rechtsdurchsetzung oder Rechtsverteidigung.

2.13 Welche Rechte haben die Betroffenen?

2.13.1 Information und Transparenz

Siehe dazu Punkt 2.8.

2.13.2 Wie schnell muss man reagieren?

Üben Betroffene ihre Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit oder Widerspruch aus, ist dem unverzüglich, längstens binnen eines Monats nachzukommen.

Nur in besonders begründeten Fällen kann diese Frist um zwei Monate, sohin auf drei Monate erstreckt werden. Allerdings sind dem Betroffenen dann innerhalb eines Monats die Gründe für die Verzögerung mitzuteilen.

2.13.3 Recht auf Auskunft

Jeder Betroffene hat das Recht, von einem Verantwortlichen (nicht aber von einem Auftragsverarbeiter) darüber Auskunft zu verlangen, ob seine personenbezogenen Daten verarbeitet werden. Ist das der Fall, sind dem Betroffenen weitere Informationen zu erteilen, etwa über den Verwendungszweck und die Empfänger seiner Daten (Art. 15 DSGVO).

Dem Betroffen ist unentgeltlich eine „Kopie der verarbeiteten Daten“ zur Verfügung zu stellen.

Der Verantwortliche muss bei einem Auskunftsersuchen vorab die Identität des Ersuchenden prüfen, zB die Übermittlung einer Passkopie zu verlangen, um nicht einer „falschen“ Person Auskunft zu erteilen und dadurch das Datengeheimnis zu brechen. Bei sensiblen Daten und sonstigen Daten mit hohem Risiko empfiehlt sich eine stärke Form der Identitätsfeststellung als die simple Vorlage einer Passkopie, zB eine Aufforderung persönlich mit Lichtbildausweis zu erscheinen („Two-Factor-Authentification“).

Auskunftsersuchen sind unentgeltlich zu erfüllen, nur bei exzessiven oder missbräuchlichen Ersuchen kann der Verwaltungsaufwand in Rechnung gestellt werden (Art. 12 DSGVO).

2.13.4 Recht auf Berichtigung

Jeder Betroffene hat das Recht, eine Berichtigung oder Vervollständigung seiner Daten zu verlangen. Wird zB der Nachname fälschlich als „Maier“ verarbeitet, kann eine Berichtigung auf „Mayer“ begehrt werden.

2.13.5 Recht auf Löschung („Vergessenwerden“)

Grundsätzlich hat jeder Betroffene das Recht, die Löschung seiner Daten zu begehren. Dieses Recht ist allerdings nicht absolut, dh dem Löschungsersuchen ist nicht in jedem Fall nachzukommen (Art. 17 DSGVO).

Eine Löschung hat im Wesentlichen nur dann zu erfolgen, wenn die Rechtsgrundlage der Verarbeitung gar nie vorhanden war oder später wegfällt, zB weil der Zweck der Verarbeitung nie erhoben wurde oder später entfällt oder weil der Betroffene eine Einwilligung widerruft oder Widerspruch erhebt (siehe zum Widerspruch Punkt 2.13.8).

Besteht eine rechtliche Verpflichtung zur Verarbeitung, zB aufgrund von Steuergesetzen, oder besteht ein bestimmtes öffentliches Interesse an der Verarbeitung, oder werden die Daten zur Verfolgung oder Verteidigung von Rechtsansprüchen benötigt, kann die Löschung unterbleiben.

Hat ein Verantwortlicher Daten „öffentlich“ gemacht, muss er die Empfänger der Daten informieren, die die Daten verarbeiten, damit auch sie die Daten löschen. Die Empfänger sind auch dem Betroffenen zu nennen.

Daten auf Backups müssen nicht sofort gelöscht werden, wenn die sofortige Löschung aus wirtschaftlichen oder technischen Gründen nicht möglich ist (§ 4 Abs. 2 DSG). Allerdings muss eine Einschränkung der Datenverarbeitung erfolgen (siehe dazu den nachfolgenden Punkt 2.13.6).

2.13.6 Recht auf Einschränkung

Einschränkung bedeutet im Wesentlichen, dass personenbezogene Daten nur mehr gespeichert werden dürfen (zB in Backups), aber sonst keine Verarbeitung erfolgen darf. Sollte es etwa erforderlich sein, Datenbanken aus einem Backup wiederherzustellen, müssen die der Einschränkung unterliegenden Daten in der wiederhergestellten Datenbank (erneut) gelöscht werden.

Ein Betroffener kann in der Regel dann eine Einschränkung verlangen, wenn der Verantwortliche eine gewisse Zeit benötigt, um etwa die bestrittene Richtigkeit von Daten zu prüfen oder wenn er die Daten nur mehr zur Verfolgung oder Abwehr von Rechtsansprüchen benötigt. Auch im Falle eines Widerspruchs hat bis zur Klärung, ob die berechtigten Interessen des Verantwortlichen überwiegen, eine Einschränkung zu erfolgen (Punkt 2.13.8).

Eine Einschränkung der Verarbeitung muss allen Empfängern von personenbezogenen Daten mitgeteilt werden (Art. 19 DSGVO).

2.13.7 Recht auf Datenübertragbarkeit (Datenportabilität)

Das Recht auf Datenübertragbarkeit bedeutet, dass der Betroffene von einem Verantwortlichen (nicht aber von einem Auftragsverarbeiter) verlangen kann, seine personenbezogenen Daten an einen anderen Verantwortlichen zu übermitteln (Art. 20 DSGVO).

Dieses Recht gilt aber nur dann, wenn alle der folgenden Voraussetzungen erfüllt sind:

> Der Betroffene hat dem Verantwortlichen seine Daten selbst aktiv zur Verfügung gestellt.
> Die Daten werden automatisiert (also nicht nur manuell) verarbeitet.
> Die Verarbeitung erfolgt entweder aufgrund einer Einwilligung oder zur Erfüllung eines Vertrages mit dem Betroffenen.

Als Beispiel könnte etwa der Wechsel des Strom- oder Handyanbieters, der Wechsel der Bank oder eines Email-Providers dienen. Auch beim Wechsel des Arbeitgebers könnte das Recht auf Datenübertragbarkeit eine Rolle spielen.

2.13.8 Widerspruchsrecht

In ganz bestimmten Fällen kann ein Betroffener Widerspruch gegen die Verarbeitung seiner personenbezogenen Daten erheben. Ein Widerspruch ist nicht mit dem Widerruf einer Einwilligung zu verwechseln.

Ein Widerspruch ist dann zulässig, wenn der Verantwortliche seine personenbezogenen Daten auf folgenden Rechtsgrundlagen (vgl Punkt 2.4.1) oder zu folgenden Zwecken verarbeitet:

> überwiegendes berechtigten Interesse,
> im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt,
> Direktwerbung (zB Email-Newsletter), oder
> Forschungs- oder statistischen Zwecken.

Bei einem Widerspruch gegen die Verarbeitung zu Zwecken der Direktwerbung und einem allenfalls damit verbundenen Profiling (siehe dazu Punkt 2.15) dürfen die Daten nicht mehr verarbeitet werden. Der Widerspruch ist quasi die gesetzliche Opt-Out-Möglichkeit.

In den anderen Fällen muss der Verantwortliche zunächst selbst abwägen, ob seine Interessen die Grundrechte und Freiheiten des Betroffenen überwiegen. Er ist dafür beweispflichtig. Überwiegen seine Interessen nicht, sind die Daten zu löschen.

Als Beispiel kann etwa die Entscheidung des EuGH iS Google Spain dienen: Google kann sich in der Regel auf ein Informationsinteresse der Öffentlichkeit berufen, allerdings ist bei einzelnen Suchergebnissen dieses öffentliche Interesse hinter die Rechte des Betroffenen zu stellen, etwa bei lange zurückliegenden nachteiligen Suchergebnissen.

Werden hingegen Daten zur Verfolgung oder der Abwehr von Rechtsansprüchen benötigt, wird das Interesse des Verantwortlichen stets überwiegen.

2.14 Bilder und Videos

Bilder und Videos, auf denen Personen erkennbar sind, gelten als personenbezogene Daten. Ihre Verarbeitung und Nutzung ist datenschutzrechtlich beschränkt.

Häufig werden in Unternehmen Mitarbeiterfotos oder Videos auf der eigenen Website oder in der Email-Signatur verwendet. Auch bei Veranstaltungen werden immer wieder Fotos von Besuchern und Teilnehmern gemacht und anschließend veröffentlicht.

Die Verarbeitung (dazu zählt auch die Veröffentlichung) von Fotos und Videos darf nur dann erfolgen, wenn sie „rechtmäßig" ist (vgl Punkt 2.4.2).

Die „Rechtmäßigkeit" lässt sich bei der Veranstaltungsfotografie in der Regel mit dem überwiegenden berechtigten Interesse des Unternehmens begründen, sofern ein größerer Personenkreis in nicht bloßstellender Art abgebildet wird. Ein Unternehmen hat schließlich ein berechtigtes Interesse, über eigene Veranstaltungen zu informieren und damit Marketing zu betreiben.

Bei Mitarbeiterfotos könnte dieser Rechtfertigungsgrund bei internen Mitarbeiterdatenbanken wegen der erleichterten internen Zusammenarbeit und bei Mitarbeiterausweisen greifen.

Bei einer anderen Nutzung von Mitarbeiterfotos, zB auf der Website oder in Social-Media-Kanälen, empfiehlt sich die Einholung einer Einwilligung. Hier ist aber besonders auf den Aspekt der „Freiwilligkeit" zu achten (vgl Punkt 2.6). Dem Mitarbeiter darf kein Nachteil aus der Verweigerung der Einwilligung erwachsen. Ebenso wenig darf der Abschluss des Dienstvertrages von der Einwilligung abhängig gemacht werden.

Für Bildaufnahmen gelten besondere Bestimmungen im österreichischen Datenschutzgesetz (§§ 12 und 13 DSG), die unter anderem Kennzeichnungs- und Löschverpflichtungen enthalten und auch die Zulässigkeit von Videoüberwachungen speziell regeln.

2.15 Profiling und automatisierte Entscheidungsfindung

Unter „Profiling" versteht die DSGVO jede automatisierte Verarbeitung personenbezogener Daten zum Zweck der Bewertung und Analyse persönlicher Aspekte des Betroffenen. Das sind zB die Arbeitsleistung, die wirtschaftliche Lage, persönliche Vorlieben und Interessen, Aufenthaltsorte und Ortswechsel.

Zusätzliche Beschränkungen gibt es, wenn das Profiling gegenüber den Betroffenen rechtliche Wirkungen entfaltet oder in ähnlicher Weise die Betroffenen erheblich beeinträchtigt.

Das ist zB dann der Fall, wenn Kreditanträge oder Bewerbungen für eine Arbeitsstelle ohne menschliches Eingreifen automatisiert bei Vorliegen bestimmter Aspekte, die sich aus dem Profiling ergeben, abgelehnt werden.

In solchen Fällen ist ein Profiling nur unter folgenden Voraussetzungen zulässig:

> Das Profiling ist für den Vertragsabschluss zwischen dem Verantwortlichen und dem Betroffenen erforderlich (zB zur Ermittlung der risikoabhängigen Kfz-Versicherungsprämie).

> Das Profiling erfolgt aufgrund einer gesetzlichen Ermächtigung oder Verpflichtung.

> Ausdrückliche Einwilligung des Betroffenen.

Bei nahezu jeder personalisierten Werbung, zB über Social Media Kanäle, wird Profiling betrieben. In der Regel wird dafür die Einwilligung des Betroffenen erforderlich sein.

Wenn ein Profiling nicht aufgrund einer gesetzlichen Ermächtigung oder Verpflichtung betrieben wird, stehen den Betroffenen folgende Rechte zu:

> Auf Wunsch des Betroffenen muss eine Überprüfung durch eine natürliche Person erfolgen.

> Der Betroffene hat das Recht, seinen Standpunkt darzulegen.

> Die automatisierte Entscheidung ist auf Antrag des Betroffenen rückgängig zu machen.

Der Betroffene ist in jedem Fall zu informieren, dass ein Profiling stattfindet. Bei einer automatisierten Entscheidungsfindung ist er auch über die dahinter liegende Entscheidungslogik zu informieren.

Bei einer umfassenden Bewertung persönlicher Aspekte der Betroffenen ist eine Datenschutz-Folgenabschätzung zwingend.

Bei jeder Art des Profiling kann der Betroffene einen Widerspruch erheben (siehe dazu Punkt 2.13.8).

2.16 Was ist zu tun, wenn etwas passiert?

2.16.1 Meldung an die Behörde

Erlangt ein Verantwortlicher (nicht jedoch ein Auftragsverarbeiter) Kenntnis von einer Verletzung des Schutzes personenbezogener Daten, hat er diese Verletzung unverzüglich, längstens jedoch binnen 72 Stunden der zuständigen Aufsichtsbehörde (siehe dazu Punkt 2.19) zu melden. Es geht darum, ob die Integrität, Vertraulichkeit und/oder Verfügbarkeit der Daten berührt ist.

Eine Ausnahme besteht dann, wenn die Verletzung mit keinem Risiko für die Betroffenen verbunden ist.

Eine Meldung muss zB dann erstattet werden, wenn eine Erpressersoftware eine (nicht durch Backup gesicherte) Kundendatenbank verschlüsselt oder wenn ein unverschlüsselter Laptop mit Kundendaten im Zug vergessen wird.

Die Meldung muss bestimmte Inhalte aufweisen (zB genaue Beschreibung, ergriffene Maßnahmen). Außerdem ist die Verletzung samt Abwehrmaßnahmen zu dokumentieren.

2.16.2 Information der Betroffenen

Besteht bei einer Verletzung nicht nur ein Risiko, sondern ein hohes Risiko für die Betroffenen, sind auch sie unverzüglich zu informieren.

Ist eine solche Information nur mit unverhältnismäßig hohem Aufwand möglich, kann die Information durch eine öffentliche Bekanntmachung oder ähnliche Maßnahme erfolgen.

2.17 Wann muss ich Daten löschen?

Personenbezogene Daten müssen dann gelöscht werden, wenn der Zweck ihrer Verarbeitung entfällt.

Dies kann sehr unterschiedlich sein. Auch können sich verschieden Löschfristen für die einzelnen Datenkategorien ein und desselben Betroffenen ergeben.

Bei Mitarbeiterdaten etwa sind Lohn- und Gehaltsdaten grundsätzlich sieben Jahre aufzubewahren. Daten, die zur Ausstellung eines Dienstzeugnisses erforderlich sind, könnten hingegen dreißig Jahre aufbewahrt werden, wenn beim Ausscheiden des Mitarbeiters kein Dienstzeugnis ausgestellt wurde. Der Anspruch

auf ein Dienstzeugnis verjährt nämlich erst nach dreißig Jahren.

Soweit Daten für die Geltendmachung oder Abwehr von Rechtsansprüchen erforderlich werden könnten, gilt im Allgemeinen eine dreijährige Verjährungsfrist (samt eines Pufferzeitraumes) für Schadenersatzklagen. In einigen Fällen könnte diese Frist aber auch dreißig Jahre betragen.

Es empfiehlt sich die Erstellung eines Löschkonzepts, auch wenn dies eine große praktische Herausforderung darstellen kann.

Die Löschung von Backups kann hinausgeschoben werden, wenn die sofortige Löschung aus wirtschaftlichen oder technischen Gründen nicht möglich ist (§ 4 Abs. 2 DSG).

2.18 Geldbußen und Schadenersatz

2.18.1 Geldbußen

Der Strafrahmen der DSGVO bewegt sich für bestimmte Verstöße zwischen € 20 Millionen oder 2% des weltweiten Vorjahres-Gesamtumsatzes oder zwischen € 40 Millionen und 4% dieses Gesamtumsatzes.

Die Bemessung der Geldbuße hängt von verschiedenen Faktoren ab: Art, Schwere und Dauer der Verletzung, Verschuldensgrad, ergriffene Abhilfemaßnahmen, Wiederholungstäterschaft, Bereitschaft zur Kooperation mit der Aufsichtsbehörde, betroffene Datenkategorien etc.

Nach dem österreichischen DSG sind auch bloße Verwarnungen möglich.

Geldbußen können sowohl gegen juristische Personen als auch unmittelbar gegen Mitglieder der Geschäftsleitung verhängt werden. Letzteres ist dann nicht zulässig, wenn ein Beauftragter gemäß § 9 Verwaltungsstrafgesetz benannt ist (das ist nicht der Datenschutzbeauftragte!).

Beim Verstoß einer Tochtergesellschaft gegen die DSGVO kann auch die Muttergesellschaft belangt werden.

2.18.2 Schadenersatz

Betroffene haben das Recht, sowohl materiellen als auch immateriellen Schadenersatz geltend zu machen.

Materielle Schäden sind Vermögensminderungen einschließlich eines entgangenen Gewinns.

Immaterielle Schäden sind solche, die sich nicht direkt im Vermögen auswirken, aber in der Regel zu einer emotionalen Beeinträchtigung führen. Denkbar sind etwa Rufschädigung, die Verbreitung sensibler Daten (zB Daten über schwere Erkrankungen) oder Diskriminierung.

Voraussichtlich wird es im Zusammenhang mit Datenschutzverletzungen auch häufig zu Sammelklagen kommen.

2.19 Die Aufsichtsbehörden

In jedem EU-Mitgliedstatt ist mindestens eine Aufsichtsbehörde einzurichten, die für den Vollzug der DSGVO im jeweiligen Land zuständig ist.

In Österreich ist dies die Datenschutzbehörde (www.dsb.gv.at) mit Sitz in Wien.

Daneben gibt es den Europäischen Datenschutzausschuss (EDSA), der aus den Leitern der nationalen Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten besteht (www.edpb.europa.eu). Er kann für die nationalen Aufsichtsbehörden bindende Leitlinien erlassen.

Betrifft eine Datenschutzangelegenheit mehrere Mitgliedstaaten, zB weil ein Konzern mit mehreren europäischen Niederlassungen involviert ist, übernimmt eine nationale Aufsichtsbehörde die Federführung für den jeweiligen Fall (One-Stop-Shop).

3 Umsetzung des Datenschutzes im Unternehmen

3.1 Vorbereitung

3.1.1 Projektmanagement

In jedem Unternehmen sollte eine bestimmte Person für die Herstellung der DSGVO-Konformität zuständig ist. Idealerweise bringt diese Person sowohl juristisches als auch technisches Verständnis mit und kennt die Abläufe im Unternehmen.

Achtung: Diese Person ist formell nicht der Datenschutzbeauftragte. Die Bezeichnung „Datenschutzbeauftragter" sollte in diesem Zusammenhang nicht verwendet werden. Der Datenschutzbeauftragte berät in Sachen Datenschutz und überwacht nur die Umsetzung der DSGVO, er ist aber nicht für die Umsetzung verantwortlich. Siehe dazu oben Punkt 2.7.

3.1.2 Beiziehung eines externen Experten

Optional kann oder sollte in komplexeren Fällen ein externer Experte beigezogen werden.

3.1.3 Bereitstellung der benötigten Ressourcen

Im Unternehmen sind ausreichende zeitliche, organisatorische und finanzielle Ressourcen bereit zu stellen. Die Umsetzung der DSGVO ist mit einigem Aufwand verbunden.

3.1.4 To-do-Liste

Weiterer Ausgangspunkt ist dann die Erstellung einer To-do-Liste samt Zeitplan für die Umsetzung (Wer macht was und bis wann?).

3.2 Erhebung des IST-Zustandes

3.2.1 Erhebung der Verarbeitungen

Zunächst sollten alle Verarbeitungen personenbezogener Daten, die im Unternehmen stattfinden, ermittelt und erhoben werden, zB Lohnverrechnung, Meldung an Sozialversicherung, Direktwerbung an Kunden, etc. Dazu könnte man sich folgender Methoden bedienen:

- Befragung der Mitarbeiter bzw der einzelnen Abteilungsleiter.
- Prüfung der registrierten Datenanwendungen laut Datenverarbeitungsregister (falls die Datenverarbeitungen im ehemaligen DVR gemeldet wurden).
- Durchsicht der Standardanwendungen.
- Durchsicht von Verträgen mit Geschäftspartnern, Kunden und Mitarbeitern.
- Prüfung der Website (Kontaktformular, Newsletter, Webshop etc.).
- Bildaufzeichnungen/Videoüberwachung (hier gelten besondere Vorschriften).

3.2.2 Datenkategorien

Als nächstes bietet sich eine Auflistung der Kategorien von verarbeiteten personenbezogenen Daten (Vorname, Name, Alter, Geschlecht, Adresse, Sozialversicherungsnummer, etc.) an.

3.2.3 Erhebung der Zwecke der Verarbeitungen

Erhebung des jeweiligen Zwecks der einzelnen Datenverarbeitungen, zB Personalverwaltung, Geschäftsabwicklung mit Kunden und Lieferanten, etc.

3.2.4 Bestimmung der jeweiligen Rechtsgrundlagen

Für jede einzelne Datenverarbeitung muss es eine Rechtfertigung geben (= Rechtmäßigkeit der Verarbeitung, siehe dazu Punkt 2.4.2). Daher muss für jede Datenverarbeitung die Rechtsgrundlage, auf der die Verarbeitung beruht, bestimmt werden. Folgende Rechtsgrundlagen kommen in Frage (dies gilt nicht für sensible Daten):

- Erfüllung eines Vertrags,
- Erfüllung einer rechtlichen Verpflichtung,

- Schutz lebenswichtiger Interessen des Betroffenen,
- Erfüllung einer Aufgabe im öffentlichen Interesse,
- Überwiegendes Interesse des Verantwortlichen oder eines Dritten gegenüber den Interessen des Betroffenen,
- Einwilligung des Betroffenen (siehe hiezu Punkt 2.9.4).

3.2.5 Sensible Daten (besondere Kategorien von Daten)

Es sollte auch geprüft werden, ob sensible Daten (zB Gesundheitsdaten, Religion, biometrische Daten etc) verarbeitet werden.

In solchen Fällen ist die Zulässigkeit der Verarbeitung an strengere Voraussetzungen geknüpft, die ebenfalls geprüft werden müssen.

3.2.6 Profiling

Profiling ist die automatisierte Datenverarbeitung zur Erstellung eines Profils über persönliche Aspekte eines Betroffenen, zB seine wirtschaftliche Lage, Gesundheit, persönlichen Vorlieben uä.

Profiling wird besonders beim Einsatz von Tracking Cookies relevant, da hier das Verhalten der Betroffenen erfasst und ausgewertet wird (zB welche Internetseiten besucht werden, was online eingekauft wird).

3.2.7 Übermittlung von Daten an Dritte und Auftragsverarbeiter

Personenbezogene Daten werden häufig an Dritte übermittelt (zB Mitarbeiterdaten an eine externe Lohnbuchhaltung). Es muss überprüft werden, ob und wann solche Übermittlungen stattfinden. Dabei ist auch folgendes zu beachten:

- Prüfung der Rechtsgrundlage (Punkt 2.4), also Prüfung, ob die Übermittlung zulässig ist.
- Besondere Voraussetzungen gelten bei Übertragung in Staaten außerhalb der EU.
- Prüfung des Vorliegens eines schriftlichen Vertrags, wenn die Übertragung zur Unterstützung des Unternehmens durch einen sogenannten „Auftragsverarbeiter“ erfolgt. Ein Muster stellt die WKO auf Ihrer Website bereit (www.wko.at/datenschutz) bereit.

3.2.8 Verpflichtung der Mitarbeiter zum Datengeheimnis

Prüfung, ob bereits eine gesetzliche oder vertragliche Verpflichtung der Mitarbeiter besteht, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses einzuhalten.

Sonst sollte eine Unterzeichnung einer Verpflichtung zur Wahrung des Datengeheimnisses durch die Mitarbeiter erfolgen.

3.2.9 Zusammenfassung der Erhebung des Ist-Zustands

- Welche Erhebungsschritte wurden konkret getätigt
- Welche Ergebnisse brachten die Erhebungen (zB sortiert nach einzelnen Datenverarbeitungen)

3.3 Erforderliche Maßnahmen

3.3.1 Verarbeitungsverzeichnis

Siehe dazu Punkt 2.9.1.

3.3.2 Technische und organisatorische Sicherheitsmaßnahmen (TOMs)

Jedes Unternehmen muss technische und organisatorische Sicherheitsmaßnahmen, die im Hinblick auf die Art der Datenverarbeitung und die Unternehmensgröße angemessen sind, einführen.

Für die technische Umsetzung sollte der externe und/oder interne IT-Betreuer beigezogen werden. Die Maßnahmen müssen dem „Stand der Technik“ entsprechen. Das bedeutet insbe-

sondere auch, dass die Maßnahmen regelmäßig evaluiert werden müssen.

Für die ebenso wichtigen organisatorischen Maßnahmen empfiehlt sich die Erstellung einer internen Datenschutzrichtlinie, in der der Umgang mit personenbezogenen Daten für die Mitarbeiter verbindlich beschrieben wird (zB „Clean Desk Policy"). Mitarbeiter sollten auch regelmäßig in Fragen des Datenschutzes geschult werden.

3.3.3 Herstellung von Transparenz

Alle Informationspflichten nach Art. 13 und 14 DSGVO müssen erfüllt werden. Die Umstände, über die Betroffene bei der Datenerhebung informiert werden müssen, sind dort genau festgelegt.

Zu den Maßnahmen zählen insbesondere auch die Erstellung einer hinreichenden Datenschutzerklärung auf der Website, Informationen auf Bestellformularen, die Information der Mitarbeiter über die Verarbeitung ihrer Daten (zB im Arbeitsvertrag) uä.

3.3.4 Wahrnehmung der Betroffenenrechte

Es sollte ein Konzept erstellt werden, wie Betroffenenrechte (zB Auskunftsverlangen) wahrgenommen werden. Dazu sollte insbesondere Folgendes gemacht werden:

> Festlegung der intern zuständigen Person.
> Festlegung des Verhaltens bei der Geltendmachung von Betroffenenrechten (Auskunft, Widerspruch, Löschung etc).
> Festlegung der zu ergreifenden Maßnahmen (Checkliste).
> Vorkehrungen treffen, dass jedem Betroffenen kurzfristig Auskunft gegeben werden kann, was das Unternehmen mit seinen Daten macht.

3.3.5 Data Breach Notification

Es sollte auch klar geregelt sein, was passiert, wenn etwas passiert (zB Hackerangriff, Verlust eines unverschlüsselten Notebooks mit personenbezogenen Daten):

> Festlegung des Verhaltens bei einer Verletzung des Schutzes personenbezogener Daten.
> Festlegung der intern zuständigen Person.
> Festlegung der zu ergreifenden Maßnahmen (Checkliste).
> Benachrichtigung der Geschäftsleitung, der Datenschutzbeauftragten, der Datenschutzbehörde und des Betroffenen

3.3.6 Verpflichtung der Mitarbeiter zum Datengeheimnis

Die Einholung einer schriftlichen Verpflichtung der Mitarbeiter zur Wahrung des Datengeheimnisses ist in der Regel notwendig. Ein Muster stellt die WKO auf Ihrer Website bereit (www.wko.at/datenschutz) bereit.

3.3.7 Vertragsprüfungen

Alle Verträge, AGBs, Datenschutzerklärungen, Einwilligungen und sonstige rechtserheblicher Dokumente sollten auf Datenschutzrelevanz (Verarbeitung personenbezogener Daten) und Datenschutzkonformität geprüft werden.

3.3.8 Datenschutz-Folgenabschätzung

Allenfalls ist die Durchführung einer Datenschutz-Folgenabschätzung notwendig.

Sie ist dann erforderlich, wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht.

3.3.9 Löschkonzept

Es ist zu empfehlen, ein Löschkonzept zu erstellen. Personenbezogene Daten dürfen nämlich nur so lange verarbeitet werden, bis der Zweck der Verarbeitung entfällt.

3.3.10 Social Media

Facebook & Co sind datenschutzrechtlich besonders vorsichtig zu handhaben, da Social Media Provider in der Regel die Daten von Usern vielfältig verwenden, insbesondere auch ein Profiling betreiben.

Auf jeden Fall sollten bei jeder Verwendung von Social Media (Fanpages, Plug-Ins) die Parametrierungen (Filtereinstellungen) überprüft und möglichst eng gehalten werden.

Außerdem wird zumindest auf der Unternehmensseite und auf der eigenen Homepage eine hinreichende Information mit Verweis auf den Social Media Provider und dessen Datenschutzerklärung erforderlich sein.

Für Anwendungen wie Facebook Pixel und Ähnliches dürfte zudem eine Einwilligung der Betroffenen erforderlich sein.

Außerdem hat der Europäische Gerichtshof (EuGH) in seinem Urteil vom 05. Juni 2018 (C-201/16) entschieden, dass Betreiber von Facebook-Fanpages mit Facebook eine gemeinsame Verantwortlichkeit für die Verarbeitung personenbezogener Daten durch Facebook trifft (siehe Punkt 2.9.6). Das heißt, der Betreiber muss mit Facebook eine Vereinbarung im Sinn des Art. 26 DSGVO abschließen.

Facebook hat auf das Urteil reagiert und eine solche Vereinbarung vorgelegt („Page Controller Addendum“) wobei offen ist, ob diese Vereinbarung den ausreichend ist (siehe: https://www.facebook.com/legal/terms/page_controller_addendum). Facebook übernimmt darin die Verantwortung für Sicherheit, Auskünfte und Information. Aber auch die Fanpage-Betreiber haben Pflichten, zB Anpassung der eigenen Datenschutzerklärung, Festlegung der Rechtsgrundlage der Verarbeitung, Weiterleitung von Anfragen Betroffener an Facebook).

3.3.11 Dokumentation

Den Verantwortlichen treffen umfassende Dokumentationspflichten in Bezug auf Datenschutz. Auf Verlangen hat er der Datenschutzbehörde die Einhaltung der Datenschutzbestimmungen nachzuweisen.

Jedes Unternehmen sollte daher eine Unterlage (auch digital möglich) erstellen, anhand derer es zu sämtlichen Aspekten des Datenschutzrechtes jederzeit Auskunft geben kann.

Aus Gründen der Lesbarkeit wird in dieser Broschüre darauf verzichtet, geschlechtsspezifische Formulierungen zu verwenden. Personenbezogene Formulierungen beziehen sich auf Frauen und Männer in gleicher Weise.

4 Checkliste

- ❍ Verantwortlichen / Team für Datenschutz bestimmen
- ❍ Erhebung des Ist-Zustandes
- ❍ Verarbeitungsverzeichnis erstellen
- ❍ Angemessenes Datenschutzniveau (TOMs)
  - ❍ Technische Maßnahmen (IT-Betreuer einschalten), zB
    - ❍ Stand der Technik
    - ❍ Virenschutz
    - ❍ Firewall
    - ❍ Aktuelle Software
    - ❍ Zugriffsberechtigungen
  - ❍ Organisatorische Maßnahmen
    - ❍ Mitarbeiterschulungen
    - ❍ interne Datenschutzrichtlinie
    - ❍ Zugangsbeschränkungen
    - ❍ Clean Desk Policy
- ❍ Transparenz
  - ❍ Datenschutzerklärung für die Website
  - ❍ Information an Mitarbeiter
  - ❍ Sonstige Bereitstellung von Information
- ❍ Einwilligungen: Prüfung, ob Einwilligungen
  - ❍ benötigt werden,
  - ❍ bereits vorhanden sind,
  - ❍ sie exakt formuliert sind.
- ❍ Auftragsverarbeiterverträge
- ❍ Drittlandübermittlungen (zB an Dienstleister zum Mailversand wie MailChimp):
  - ❍ Prüfung der Zulässigkeit
- ❍ Datenschutzfolgenabschätzung
- ❍ Verpflichtungserklärung für Mitarbeiter zur Wahrung des Datengeheimnisses
- ❍ Löschkonzept
- ❍ Konzept zur Wahrnehmung von Betroffenenrechten
- ❍ Konzept über Vorgehensweise bei Verletzungen des Datenschutzes
- ❍ Hinreichende Dokumentation

Ein Team von Spezialisten für fast alle Rechtsgebiete

Die Rechtsanwaltskanzlei Greiter Pegger Kofler & Partner geht auf Dr. Josef Greiter zurück, der im September 1897 seine Kanzlei eröffnete. Seit damals schenken uns Klienten ihr Vertrauen. Wir verstehen uns heute als modernes, aus der Tradition gewachsenes Dienstleistungsunternehmen, das Klienten mit einem Team von Spezialisten in fast allen Rechtsgebieten berät und vertritt.

Unser Team besteht aus ca. 35 Mitarbeiterinnen und Mitarbeitern, davon derzeit 11 Rechtsanwälten. Einer unserer Schwerpunkte ist das Wirtschaftsrecht, wobei wir auch international tätige Klienten betreuen.

Der Blick über die eigenen Grenzen ist für uns eine Selbstverständlichkeit. Wir verfügen daher über ein Netzwerk persönlicher Kontakte zu Anwälten in fast allen Ländern und korrespondieren in den vier Sprachen Deutsch, Englisch, Französisch und Italienisch. Unsere vielfältige Erfahrung und unser Wissen geben wir durch Vortragstätigkeiten, insbesondere an Hochschulen und Universitäten, weiter.

Greiter
Pegger
Kofler

Rechtsanwälte

Greiter Pegger Kofler & Partner
Rechtsanwälte

Maria-Theresien-Straße 24
6020 Innsbruck, Austria

Telefon: +43 512 57 18 11
Fax: +43 512 58 49 25

office@lawfirm.at
www.lawfirm.at