Information zum Datenschutz

Kompakter Überblick rund um das Thema Datenschutz in der betrieblichen Praxis

Gerald Langeder
Geschäftsführer & Gesellschafter
(Consulting, Coaching, Architektur & Lösungen)
Zertifizierter Datenschutzbeauftragter

GEN•ICT
Hamberg 45
A - 4201 Gramastetten
UID: ATU72049017

www.genict.com
Xing
LinkedIn

Sehr geehrte Kundin/Mitarbeiterin,
sehr geehrter Kunde/Mitarbeiter,

in vielen Bereichen der betrieblichen Praxis werden Computer und Datenverarbeitungssysteme eingesetzt, um damit Daten zu verarbeiten. Dabei ist unser Unternehmen stets darauf bedacht, die einschlägigen Bestimmungen zum Datenschutz einzuhalten. Auch Sie können hierzu Ihren Beitrag leisten. Mit Ihnen schaffen wir es, dass der Datenschutz in unserem Unternehmen auf einem hohen Niveau gehalten werden kann. Mit dieser Informationsbroschüre können Sie sich ein Bild davonmachen, worum es beim Thema Datenschutz geht. Sie erhalten Antworten auf die häufigsten Fragen zur Zulässigkeit der Verarbeitung personenbezogener Daten nach der VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – kurz Datenschutz-Grundverordnung (DS-GVO).
Sollten Sie darüber hinaus Fragen zum Datenschutz haben, dann sprechen Sie mich gerne persönlich an.

Mit freundlichen Grüßen
Gerald Langeder
(Ihr Datenschutzbeauftragter)

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

Inhaltsverzeichnis

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

1. Datenschutz – was dahintersteckt

Welchen Zweck haben der Datenschutz und die DSGVO?

Der europäische Gesetzgeber bekennt sich mit der DSGVO (Erwägungsgrund 1) klar zur Charta der Grundrechte der Europäischen Union, welche in den Art. 7 und 8 das Recht auf Achtung des Privat- und Familienlebens sowie das Recht auf Schutz personenbezogener Daten regelt. Die DSGVO schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. Sie schützt also natürliche Personen vor der Beeinträchtigung ihrer Persönlichkeitsrechte, sofern deren personenbezogene Daten verarbeitet werden. Die wesentliche Idee bzw. das Ziel des Datenschutzes ist es, den sogenannten „gläsernen Menschen“ zu verhindern: Jeder Mensch soll grundsätzlich selbst entscheiden können, wem wann welche seiner persönlichen Daten zugänglich sein sollen.

Was bedeutet Persönlichkeitsrecht?

Das Allgemeine Persönlichkeitsrecht ist im Grundgesetz geregelt (Art. 2 Abs. 1 GG). Es räumt jedem Einzelnen das Recht auf

- Individualsphäre (Schutz des Selbstbestimmungsrechts, z. B. Recht auf informationelle Selbstbestimmung),
- Privatsphäre (Leben im häuslichen Bereich, Privatleben, z. B. Verletzung bei unverlangter E-Mail-Zusendung) und
- Intimsphäre (innere Gedanken- und Gefühlswelt) ein.

Die Charta der Grundrechte der Europäischen Union führt diese Rechte ebenfalls auf.

Was beinhaltet das Recht auf informationelle Selbstbestimmung?

Das sogenannte Recht auf informationelle Selbstbestimmung gehört zum Allgemeinen Persönlichkeitsrecht. Die informationelle Selbstbestimmung ist das Recht des Einzelnen, selbst über die Preisgabe und

Verwendung seiner personenbezogenen Daten zu bestimmen. So bleibt es beispielsweise jedem selbst überlassen, ob er Informationen über sich im Internet veröffentlicht oder nicht. Werden gegen seinen Willen solche Veröffentlichungen gemacht, kann er dagegen vorgehen, da sein Recht auf informationelle Selbstbestimmung verletzt wurde.

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

Wo findet man gesetzliche Regelungen zum Datenschutz?

Der Gesetzgeber hat in verschiedenen Gesetzen Bestimmungen aufgenommen, die den Datenschutz regeln. Das wichtigste Gesetz ist dabei die VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – kurz Datenschutz-Grundverordnung (DS-GVO).

Als EU-Verordnung gilt sie als vorrangiges Recht vor allen nationalen gesetzlichen Regelungen. Nationale Regelungen dürfen die DS-GVO lediglich spezifizieren, konkretisieren oder ergänzen, sofern die DS-GVO eine solche Spezifizierung oder Konkretisierung ausdrücklich zulässt bzw. keine Regelungen dazu trifft. Man spricht im Zusammenhang der Spezifizierungen oder Konkretisierungen auch von sogenannten Öffnungsklauseln.

Darüber hinaus gibt es noch andere Gesetze, die Vorgaben machen, wie mit personenbezogenen Daten umgegangen werden darf. Beispielsweise wird auch durch Regelungen im Telekommunikationsgesetz (TKG), Telemediengesetz (TMG) oder in den Sozialgesetzbüchern (SGB) der Datenschutz gewährleistet. Auch die Katholische und Evangelische Kirche haben sich eigene Regelungen zum Umgang mit personenbezogenen Daten

gegeben, welche aber mit den Regelungen der DS-GVO in Einklang zu stehen haben. Im Übrigen kann auch beispielsweise in Betriebsvereinbarungen geregelt sein, was im Unternehmen hinsichtlich des Umgangs mit personenbezogenen Daten der Beschäftigten zu beachten ist.

Muss ein Unternehmen alle Datenschutzgesetze berücksichtigen?

Ob und inwieweit ein Unternehmen alle Datenschutzgesetze beachten muss, hängt davon ab, wie das Unternehmen organisiert ist. Für ein privatrechtliches Unternehmen gilt grundsätzlich die DSGVO. Für den Kindergarten einer Kirchengemeinde gilt hingegen das kirchliche Datenschutzrecht. Öffentliche Stellen, wie z. B. eine Stadtverwaltung, unterliegen den datenschutzrechtlichen Regelungen der DSGVO.

Gibt es in anderen Staaten ähnliche Gesetze?

Die Mitgliedstaaten der Europäischen Union unterliegen alle der DSGVO. Im Gegensatz zur früher gültigen EU-Datenschutzrichtlinie (Richtlinie 95/46/EG), welche von den Mitgliedstaaten in nationales Recht umgesetzt werden musste, gilt sie unmittelbar in jedem Mitgliedstaat. Dadurch wird ein erheblich einheitlicheres Datenschutzrecht in Europa erreicht.

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

Welche Daten werden durch die DSGVO geschützt?

Nicht alle Daten werden von der DSGVO erfasst. Nur wenn diese Daten personenbezogen sind, fallen sie in den Anwendungsbereich der DS-GVO. Was unter „personenbezogen“ zu verstehen ist, legt die DS-GVO ebenfalls fest. Nach Art. 4 Abs. 1 sind dies alle Informationen über eine identifizierte oder identifizierbare natürliche Person, die sogenannte betroffene Person. Identifizierbar ist eine natürliche Person dann, wenn die vorliegenden Informationen einzeln oder in Kombination miteinander dazu geeignet sind, Rückschlüsse auf die natürliche Identität der betroffenen Person zu ziehen.

Was sind personenbezogene Daten?

Typische personenbezogene Daten sind Name, Adresse, Telefonnummer, Geburtsdatum, Foto, E-Mail-Adresse, Arbeitsverhalten, Kfz-Kennzeichen, Gesundheitsinformationen und anderes. Letztlich alle Daten, die die betroffene Person, deren Verhalten oder Lebensumstände beschreiben. Haben die Informationen keine eindeutige Zuordnung zu einer natürlichen Person und kann diese Zuordnung zudem nicht hergestellt werden, weil sie beispielsweise anonymisiert wurden, dann fällt die Verarbeitung solcher Daten nicht unter die DSGVO.

Sind Firmendaten auch personenbezogen?

Daten von juristischen Personen, also z. B. Daten einer AG, GmbH oder GmbH & Co. KG, werden von der DS-GVO nicht erfasst. Anders sieht dies aus, wenn ein Unternehmen aus einer Personengesellschaft besteht. In der Regel handelt es sich z. B. bei einem Malerfachgeschäft, einer Metzgerei oder einem Hausmeisterservice um eine Personengesellschaft und somit um natürliche Personen, deren personenbezogene Daten durch die DS-GVO geschützt sind. Auch die personenbezogenen Daten von Ansprechpartnern, beispielsweise in einer AG oder einer GmbH, fallen unter die Bestimmungen der DS-GVO.

Vorsicht: Auch die personenbezogenen Daten einer Ein-Personen-GmbH fallen unter die DS-GVO, obwohl es sich um eine Kapitalgesellschaft handelt.

Gilt die DS-GVO auch im privaten Umfeld?

Die Verarbeitung von personenbezogenen Daten für ausschließlich persönliche oder familiäre Tätigkeiten fällt nicht unter die Vorgaben der DSGVO.

Beispiel:

Wenn Sie privat ein elektronisches Adressbuch nutzen, brauchen Sie nicht die Vorgaben der DSGVO zu beachten. Anders wäre dies etwa dann zu beurteilen, wenn Sie eine CD zum Verkauf anbieten möchten, auf der diese Adressdaten enthalten sind. Dann handeln Sie nicht mehr für ausschließlich persönliche und familiäre Zwecke. In einem solchen Fall müssten Sie die Bestimmungen der DS-GVO berücksichtigen.

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

Ist auch Datenverarbeitung mit Papier und Bleistift von der DSGVO erfasst?

Besonders einfach und effektiv sind natürlich personenbezogene Daten zu verarbeiten, wenn sie in elektronischer Form vorliegen, doch bedeutet dies nicht, dass der Schutz der DSGVO nicht auch nicht digitale Daten umfasst. Personenbezogene Daten sollen unabhängig von der verwendeten Technik geschützt werden. Daher sind personenbezogene Daten, welche nicht digital erfasst sind, sich aber in einem nicht digitalen Dateisystem mit geordneten Kriterien befinden oder aber für die Überführung in ein digitales Dateisystem bestimmt sind, ebenfalls von den Regelungen der DS-GVO erfasst. Werden personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen erhoben, verarbeitet oder genutzt, dann spricht man von automatisierten Verarbeitungen. Die dabei zum Einsatz kommenden Computer und Datenverarbeitungsanlagen bergen vielerlei Risiken für die verarbeiteten personenbezogenen Daten. So können Daten unzulässigerweise verknüpft oder ausgewertet werden. Obwohl dies beispielsweise bei einer Auswertung mit Papier und Bleistift nicht so einfach geht, sind Datenverarbeitungen ohne den Einsatz von Computern und anderen Datenverarbeitungsgeräten grundsätzlich auch von der DS-GVO erfasst, sofern diese Daten entsprechende Ordnungskriterien haben.

Nicht automatisierte Verarbeitung

Bei einer nicht automatisierten Verarbeitung handelt es sich um eine Sammlung von Daten, die man nach bestimmten Merkmalen oder Kriterien ordnen oder auswerten kann.

> Typische sind die geordnete Aufbewahrung von Lohnsteuerkarten in einem Unternehmen oder die bei einer Behörde manuell geführte Kartei.

Sind alle personenbezogenen Daten gleich?

Die DS-GVO kennt personenbezogene Daten, die besonders schützenswert sind. Diese dürfen nur unter ganz bestimmten Voraussetzungen verarbeitet werden. Welche Daten darunterfallen, ist in Art. 9 DSGVO festgelegt. Danach zählen zu den sogenannten besonderen Kategorien personen-bezogener Daten Angaben über

- die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,
- die Gewerkschaftszugehörigkeit,
- genetischen Daten,
- biometrischen Daten,
- Gesundheitsdaten sowie
- Daten zum Sexualleben oder der sexuellen Orientierung.

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

Sollen solche Daten verarbeitet werden, ist, von den Ausnahmen gemäß Art. 7 Abs. 7 lit. b–j abgesehen, eine besondere Einwilligung nach Art. 7 DS-GVO und den dazugehörigen Erwägungsgründen erforderlich.

Aber auch „normale“ personenbezogene Daten können zu besonderen Arten personenbezogener Daten werden. Dies hängt oftmals davon ab, in welchem Zusammenhang die Daten verwendet werden. Die Anschrift einer Person ist zwar prinzipiell wenig bedenklich. Allerdings kann die Anschrift eines Patienten in einer psychiatrischen Klinik einen Hinweis auf dessen Gesundheitszustand geben.

2. Verarbeitung von Daten

Was bedeutet Verarbeiten?

In der DSGVO umfasst der Begriff eine Vielzahl von Tätigkeiten, welche automatisiert oder nicht automatisiert an oder mit personenbezogenen Daten durchgeführt werden. Dabei bedeuten: Erheben – das Beschaffen von Daten über eine natürliche Person (Betroffener), z. B. die Angaben in einem Formular, das Befragen von Passanten für eine Umfrage oder die Angaben auf einem Preisausschreiben Erfassen – das Überführen der erfassten Daten in ein relevantes Dateisystem Organisieren und Ordnen – das Zuordnen von Sortier- und Suchkriterien sowie deren geordnete Verwendung im Dateisystem Speichern – das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger, um diese weiterzuverarbeiten oder diese zu nutzen Anpassen oder Verändern – das inhaltliche Umgestalten gespeicherter personenbezogener Daten (Beispiel: Sie ändern die E-Mail-Adresse eines Kunden im elektronischen Adressbuch, weil dieser sich eine neue zugelegt hat) Auslesen, Abfragen oder Verwenden –jede Form der Darstellung und Nutzung der gespeicherten personenbezogenen Inhalte. Dies kann z. B. am Bildschirm oder durch Ausgabe in Listen oder Dateien erfolgen. Übermitteln, Verbreitung oder eine andere Form der Bereitstellung – das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte diese einsieht oder abruft (Beispiel: Sie geben einem Hotel den Namen eines Mitarbeiters, um so ein Zimmer für die Dienstreise dieses Mitarbeiters zu reservieren) Abgleich oder Verknüpfung – Vergleichen, Verknüpfen oder Zusammenführen von personenbezogenen Datensätzen anhand eindeutiger Kriterien Einschränken – das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung zu sperren Löschen – das nicht wiederherstellbare Entfernen gespeicherter personenbezogener Daten Vernichten– das nicht wiederherstellbare Vernichten nicht automatisiert verarbeiteter personenbezogener Daten bzw. von Datenträgern, auf welchen personenbezogene Daten gespeichert sind.

Wann ist die Verarbeitung personenbezogener Daten erlaubt?

Die DS-GVO ist vom sogenannten „Erlaubnisvorbehaltsprinzip“ geprägt. Dieses Prinzip besagt, dass die Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist. Dies ist nur dann erlaubt, wenn es eine entsprechende Rechtsgrundlage gibt. Diese kann sich aus der DS-GVO, einer anderen (vorrangigen) Rechtsvorschrift oder der Einwilligung des Betroffenen ergeben.

Was ist unter einer Einwilligung zu verstehen?

Mit einer sogenannten Einwilligung verleiht der Betroffene seinem freien Willen Ausdruck, dass er mit der Verarbeitung seiner personenbezogenen Daten für einen bestimmten Zweck einverstanden ist. Die Einwilligung muss zeitlich immer vor dem Beginn der Verarbeitung erfolgen.

Wann ist eine Einwilligung wirksam erteilt?

Die DSGVO sieht in Art. 7 und den dazugehörigen Erwägungsgründen vor, dass eine Einwilligung nur unter bestimmten Voraussetzungen wirksam von einem Betroffenen erklärt werden kann:

- Die Einwilligung erfolgt freiwillig.
- Sie gilt für einen konkreten Fall und sollte nicht mit anderen Einwilligungen gekoppelt werden.
- Sie muss für die einwilligende Person klar und verständlich formuliert sein.
- Sie muss den Zweck der beabsichtigten Datenverarbeitung erkennen lassen.
- In unterschiedliche Verarbeitungszwecke ist jeweils einzeln einzuwilligen.
- Die Widerrufsmöglichkeit muss der einwilligenden Person vor der Einwilligung mitgeteilt werden.
- Sie muss aktiv durch eine eindeutige Handlung erfolgen (Opt-in). Wenn die Einwilligung beispielsweise vorgegeben ist und der Betroffene durch Durchstreichen oder Entfernen eines Hakens quasi erst seine Einwilligung verneinen müsste, dann ist eine auf diese Weise erlangte Einwilligungserklärung unwirksam. Dies hat zur Folge, dass die spätere Verarbeitung oder Nutzung der erhaltenen personenbezogenen Daten unzulässig ist.
- Der Verarbeitende muss die Einwilligung nachweisen können.

Beispiel für eine Einwilligungserklärung für die Versendung von Werbung

- Ja, ich bin damit einverstanden, dass meine Adresse genutzt wird, um mir in unregelmäßigen Abständen Informationen und Prospekte zu neuen Produkten aus dem Hause Mustermann zukommen zu lassen. Diese Einwilligung kann ich jederzeit per Post, Telefon, Fax oder E-Mail widerrufen.

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

Wie muss eine Einwilligungserklärung optisch gestaltet sein?

Folgende Punkte sind bei der Gestaltung von Einwilligungserklärungen zu beachten:

- Die Einwilligungserklärung darf nicht irgendwo versteckt sein.
- Sie muss optisch hervorgehoben werden, wenn sie in Zusammenhang mit anderen Erklärungen abgegeben wird. Aus diesem Grund ist es beispielsweise unzulässig, wenn eine Einwilligung in die Verarbeitung von personenbezogenen Daten in den Allgemeinen Geschäftsbedingungen (AGB) versteckt wird. So könnte es passieren, dass ein Betroffener nicht bemerkt, dass er eingewilligt hat.

Gilt eine Einwilligung für immer und ewig?

Eine Einwilligung in die Verarbeitung von personenbezogenen Daten ist insbesondere auch dadurch gekennzeichnet, dass sie widerrufen werden kann. Macht ein Betroffener von diesem Widerrufsrecht Gebrauch, dann dürfen seine personenbezogenen Daten für die Zukunft grundsätzlich nicht mehr verarbeitet werden.

Eine Verarbeitung oder Nutzung gegen den Willen des Betroffenen ist unzulässig!

Muss man volljährig sein, um einwilligen zu können?

Die DS-GVO sieht vor, dass, wenn ein Kind bei einem Angebot von Diensten der Informations-gesellschaft einwilligen soll, dieses das 16. Lebensjahr vollendet haben muss (Art. 8 DS-GVO). Ansonsten ist die Einwilligung vom Träger der elterlichen Verantwortung abzugeben. Allerdings können Mitgliedstaaten per Rechtsvorschrift eine niedrigere Altersgrenze, jedoch mindestens das vollendete 13. Lebensjahr, festlegen. Ohne gesetzliche Festlegung in Deutschland kann man hier ähnlich wie im Strafrecht jedoch auf die Einsichtsfähigkeit abstellen. Danach kann grundsätzlich von einem 14-Jährigen erwartet werden, dass er die Folgen seines Handelns abschätzen kann.

Allerdings hängt die Einsichtsfähigkeit von vielerlei Faktoren ab, z.B.:

- schwer zu erfassender oder komplizierter Sachverhalt
- Erfahrenheit der einwilligenden Person im Geschäftsleben (Jugendliche kennen nicht zwangsläufig die Funktion einer Kreditauskunft)
- Umstände, wann, wie und wo die Einwilligung erklärt werden soll (die Einholung einer Einwilligung auf einer Party kann z.B. ggf. unzulässig sein) Auf der sicheren Seite ist man allerdings, wenn zusätzlich die Einwilligung eines Erziehungsberechtigten eingeholt wird.

Wie kann man im Internet einwilligen?

Über das Internet lässt sich heutzutage vielerlei auch elektronisch erledigen. Egal ob Bestellungen, Gewinnspiele oder das Abonnieren eines E-Mail-Newsletters, ohne die Angabe von personenbezogenen Daten lassen sich diese Vorhaben kaum abwickeln.

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

Damit ein Unternehmen diese Daten erheben, verarbeiten oder nutzen darf, muss die jeweilige Person diesbezüglich einwilligen. Allerdings lässt sich nur umständlich eine schriftliche Einwilligungserklärung einholen.

Daher hat der Gesetzgeber beispielsweise im Telemediengesetz auch Regelungen zur sogenannten elektronischen Einwilligung vorgesehen:

- Es muss sichergestellt sein, dass die Einwilligung eindeutig und bewusst abgegeben wurde. Achten Sie z. B. darauf, wenn Sie selbst einen E-Mail-Newsletter erstellen und verschicken wollen, dass ein Kästchen mit einem Häkchen vorgesehen ist, welches der Kunde anklicken muss, und erst dann seine Einwilligung erteilt.
- Achten Sie außerdem darauf, dass diese Einwilligungserklärung systemseitig protokolliert wird. Das heißt, es muss jederzeit die Möglichkeit bestehen, den Einwilligungstext einzusehen und die Einwilligungserklärung zu widerrufen.

Der Inhalt der elektronischen Einwilligung muss jederzeit abrufbar sein. Die elektronische Einwilligung muss jederzeit mit Wirkung für die Zukunft widerrufen werden können.

Darf ein Unternehmen auch ohne Einwilligung personenbezogene Daten verarbeiten?

Neben der Zulässigkeit der Datennutzung aufgrund einer rechtlichen Vorschrift oder einer Einwilligung wurde in der DS-GVO eine weitere Rechtsgrundlage geschaffen, wonach personenbezogene Daten für eigene Geschäftszwecke erhoben, verarbeitet oder genutzt werden dürfen (Art. 6 Abs. 1 lit. b). Nach dieser Vorschrift ist dies auch ohne ausdrückliche Einwilligung zulässig, wenn z.B.

- Die personenbezogenen Daten zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich sind, sofern die betroffene Person eine der Vertragsparteien ist. Ein typisches Beispiel sind hier Lieferadressen, denn ohne diese könnten die Lieferung und damit die Erfüllung eines Kaufvertrags nicht erfolgen. Ein weiteres Beispiel sind die Informationen über einen Betroffenen, die ein Reisebüro an das gebuchte Hotel weitergibt, damit eine Reise stattfinden kann.
- Das Interesse des Unternehmens an der Datenverarbeitung oder -nutzung dasjenige der betroffenen Person überwiegt. Diese Interessenabwägung ist unter anderem in Art. 6 Abs. 1 lit. f vorgesehen.

Beispiel für eine elektronische Einwilligungserklärung, bei der durch das Setzen des Häkchens der Wille zum Ausdruck gebracht wird:

- ○ Ich habe die Allgemeinen Geschäftsbedingungen (AGB) sowie die Datenschutzgrundsätze gelesen und erkenne diese an.
- ○ Ja, ich möchte per E-Mail über neue Softwareprodukte und Updates informiert werden. Den Newsletter kann ich jederzeit abbestellen. Ein entsprechender Link befindet sich in jeder Newsletter-Ausgabe bzw. auf der Homepage.

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

3. Datenschutz im Unternehmen

Wessen personenbezogene Daten müssen im Unternehmen geschützt werden?

Alle Daten, die personenbezogen sind, fallen unter die Bestimmungen der DSGV0. Im Unternehmen sind daher nicht nur die Daten der **Mitarbeiter** zu schützen. Auch die Daten von **Bewerbern**, **Kunden** oder **Lieferanten und Dritte** unterliegen den gesetzlichen Regelungen, wenn der Bezug zu einer natürlichen Person hergestellt werden kann.

Wird die Einhaltung des Datenschutzes von staatlicher Seite kontrolliert?

Für die Kontrolle des Datenschutzes gibt es sogenannte Aufsichtsbehörden für den Datenschutz. Diese können schriftlich Auskunft zur Verarbeitung personenbezogener Daten von einem Unternehmen verlangen. Aber auch unangemeldete Kontrollen im Unternehmen vor Ort können notwendig sein, um die Umsetzung der datenschutzrechtlichen Bestimmungen zu kontrollieren. Die zuständige Datenschutzaufsichtsbehörde kümmert sich auch um Beschwerden von Betroffenen, die ihr Persönlichkeitsrecht beispielsweise durch die Verarbeitung ihrer personenbezogenen Daten verletzt sehen. Zur Durchsetzung der datenschutzrechtlichen Bestimmungen sind einer Aufsichtsbehörde nach Art. 58 DS-GVO weitreichende Befugnisse eingeräumt. Stellt die Aufsichtsbehörde schwerwiegende Verstöße oder Mängel fest, kann sie deren Abstellung anordnen, ein Bußgeld verhängen und die Verarbeitung personenbezogener Daten oder einzelner Datenverarbeitungsverfahren untersagen.

Wer ist im Unternehmen für die Einhaltung des Datenschutzes verantwortlich?

Wenn ein Unternehmen personenbezogene Daten erhebt, verarbeitet oder nutzt, dann trägt es hierfür die Verantwortung. Ein solches Unternehmen nennt man dann auch den Verantwortlichen (Art. 4 Abs. 7 DS-GVO). Weil es sich bei Unternehmen oft um juristische Personen handelt, muss die Geschäftsleitung für die Einhaltung der gesetzlichen Regelungen sorgen. Diese vertritt nämlich das Unternehmen nach außen und ist somit für die Einhaltung des Datenschutzes verantwortlich.

Wer kontrolliert den Datenschutz im Unternehmen?

Eine Kontrollfunktion im Unternehmen nimmt der betriebliche Datenschutzbeauftragte wahr. Im Rahmen seiner Aufgaben (Art. 39 DS-GVO) wirkt er darauf hin, dass die Regelungen zum Datenschutz eingehalten und umgesetzt werden. In dieser Funktion unterstützt er die Geschäftsleitung, welche letztendlich alle erforderlichen Entscheidungen im Hinblick auf die Einhaltung der gesetzlichen Bestimmungen trifft und verantwortet.

Warum sollten Mitarbeiter eine Verpflichtungserklärung unterschreiben?

Der Gesetzgeber schreibt in Art. 29 DS-GVO, dass der Verantwortliche sicherzustellen hat, dass die ihm unterstellten Personen, die Zugang zu personenbezogenen Daten haben, diese Daten

ausschließlich auf Weisung des Verantwortlichen verarbeiten dürfen. Diese Verpflichtung der Mitarbeiter wird sinnvollerweise schriftlich vorgenommen, damit der Verantwortliche bei Bedarf gegenüber einer Aufsichtsbehörde für den Datenschutz nachweisen kann, dass dies auch tatsächlich geschehen ist.

Wie lange gilt diese Verpflichtung?

Die Verpflichtung zur Verschwiegenheit und ordnungsgemäßen Verarbeitung personenbezogener Daten entfaltet nicht nur während Ihrer Tätigkeit für das Unternehmen Wirkung. Auch nach Ende Ihrer Beschäftigung gilt sie fort. Das bedeutet, dass Ihnen auch danach eine unberechtigte Verarbeitung von personenbezogenen Daten verboten ist.

Welche Rechte hat ein Betroffener?

Die DS-GVO regelt auch, welche Rechte jede betroffene Person im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten geltend machen kann. Ein besonderes Ziel der DS-GVO ist es, die Rechte der betroffenen Person zu stärken, und so beschäftigen sich gleich mehrere Artikel mit diesen Rechten. Niemand darf daran gehindert werden, diese Rechte auszuüben. Ferner können diese Rechte weder durch eine Vertragsbedingung noch durch Kollektivvereinbarungen ausgeschlossen werden. Das gleiche gilt selbst für Gesetze der Mitgliedsstaaten.

Recht auf transparente Information und Kommunikation (Art. 12 DS-GVO)

Alle Informationen und alle Mitteilungen an die betroffene Person müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung stehen. Dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Information kann schriftlich, elektronisch oder auf Wunsch mündlich stattfinden. Die Information muss in der Regel innerhalb eines Monats erfolgen und ist unentgeltlich zur Verfügung zu stellen.

Recht auf Auskunft (Art. 15 DS-GVO) - reaktive Information

Alle betroffenen Personen können darüber Auskunft verlangen, welche Daten zu ihrer Person wie und wozu verarbeitet werden, woher sie stammen und wohin sie übermittelt werden, wie lange diese Daten voraussichtlich verarbeitet werden (sofern möglich). Über eingehende Auskunftsersuchen sind umgehend Geschäftsleitung und Datenschutzbeauftragter zu informieren, denn bei schuldhafter Verzögerung drohen Bußgelder von bis zu 20.000.000 €.

Recht auf Information (Art. 13 D5-GVO) - aktive Information

Darüber hinaus regelt die DS-GVO insbesondere auch die Informationspflichten des Verantwortlichen gegenüber der betroffenen Person. Werden personenbezogene Daten bei der betroffenen Person erhoben, muss der Verantwortliche die betroffene Person aktiv informieren, sofern die Information der betroffenen Person nicht bereits vorliegt. Folgendes muss die Information enthalten:

- Name und Kontaktdaten des Verantwortlichen, ggf. seines Vertreters
- die Kontaktdaten des Datenschutzbeauftragten
- die Verarbeitungszwecke
- die Rechtsgrundlage der Verarbeitung
- die berechtigten Interessen des Verantwortlichen, sofern eine Interessensabwägung stattfand
- die Empfänger der Daten, insbesondere wenn sie in Drittstaaten ansässig sind
- ggf. sind Nachweise über die Sicherheit beim Empfänger oder aber eine Bezugsquelle zu diesen Nachweisen zu erbringen.
- die voraussichtliche Speicherdauer bzw.
- die Kriterien zur Festlegung, wenn diese nicht konkret genannt werden kann
- Hinweis auf das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch und die Datenübertragbarkeit
- Hinweis auf die Widerrufbarkeit der Einwilligung, sofern die Einwilligung die Rechtsgrundlage ist
- Hinweis auf das Bestehen eines Beschwerderechtes bei einer Aufsichtsbehörde
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist
- ob die betroffene Person zur Bereitstellung der Daten verpflichtet ist und welche Folgen die Nichtbereitstellung hätte
- bei automatisierter Entscheidungsfindung/Profiling, die dahinterstehende Logik und die möglichen Auswirkungen für die betroffene Person
- Ist eine Zweckänderung geplant, muss vor der Weiterverarbeitung der betroffenen Person der neue Zweck mitgeteilt werden.
- Wurden die personenbezogenen Daten nicht bei der betroffenen Person erhoben, unterliegt der Verantwortliche der Pflicht, folgende Informationen an die betroffene Person zu melden, sofern diese der betroffenen Person nicht bereits bekannt sind:
- alle Informationen, die bei Erhebung bei der betroffenen Person erforderlich sind mit Ausnahme der Information über die Erforderlichkeit der Bereitstellung und Folgen der Nicht-Bereitstellung die Quelle, aus welcher die Information stammt

Handelt es sich bei den personenbezogenen Daten um Daten zur Kommunikation mit der betroffenen Person, erfolgt die Information spätestens zum Zeitpunkt der ersten Mitteilung. Ist die Offenlegung an einen anderen Empfänger beabsichtigt, erfolgt sie spätestens zum Zeitpunkt der ersten Offenlegung.

Recht auf Berichtigung (Art. 16 DS-GVO)

Sind personenbezogene Daten einer betroffenen Person fehlerhaft, hat die betroffene Person das Recht, dass der Verantwortliche und auch mögliche Datenempfänger, die diese Daten vom Verantwortlichen übermittelt bekommen haben, diese Daten anhand der Angaben der betroffenen Person korrigieren.

Recht auf Löschung = Recht auf Vergessenwerden" (Art. 17 DS-GVO)

Sofern die weitere Verarbeitung der personenbezogenen Daten der betroffenen Person nicht erforderlich ist, kann die betroffene Person die Löschung ihrer personenbezogenen Daten beim Verantwortlichen und den möglichen Datenempfängern verlangen. Ein Hinderungsgrund wären z. B. steuerrechtliche Aufbewahrungspflichten bei Kaufverträgen. Solche Aufbewahrungspflichten finden sich beispielsweise im Steuerrecht. Dort wird beispielsweise festgelegt, dass Belege 10 Jahre lang aufbewahrt werden müssen.

Das Recht auf Löschung betrifft auch die Speicher- oder Verarbeitungsdauer von personenbezogenen Daten. Fällt die Zweckbindung oder die Rechtsgrundlage der Verarbeitung weg, ist die weitere Verarbeitung unzulässig und die Daten müssen gelöscht (zumindest aber anonymisiert) werden. Beispielsweise wären die Anschriftendaten aus einem Preisausschreiben dann zu löschen, wenn der Gewinn an den Gewinner übergeben wurde und damit das Preisausschreiben abgeschlossen ist.

Nachdem eine Aufbewahrungsfrist abgelaufen ist, müssen die personenbezogenen Daten endgültig gelöscht oder anonymisiert werden.

Recht auf Einschränkung (Art. 18 DS-GVO)

Wenn die Löschung der personenbezogenen Daten nur schwer möglich oder die weitere Speicherung erforderlich ist, besteht die Möglichkeit, diese Daten einzuschränken. Hierbei werden die entsprechenden Daten gekennzeichnet, sodass sie von zukünftigen Verarbeitungen ausgeschlossen werden. Dies kann z.B. durch den Vermerk „Gesperrt" im Datensatz erfolgen. Auch hier gilt, dass dieses Recht nur anwendbar ist, wenn die weitere Verarbeitung nicht erforderlich ist.

Recht auf Widerspruch (Art. 21 DS-GVO)

Die betroffene Person kann gegen die weitere Verarbeitung ihrer personenbezogenen Daten Widerspruch einlegen. Der Verantwortliche verarbeitet daraufhin die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder aber die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Das Widerspruchsrecht gilt insbesondere gegen Direktwerbung (Abs. 2), die aufgrund des Widerspruchs zu unterlassen ist.

Recht auf Datenübertragbarkeit (Art. 20 DS-GVO)

Jede betroffene Person kann die Herausgabe ihrer personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format verlangen. Dies betrifft alle personenbezogenen Daten, welche die betroffene Person dem Verantwortlichen zur Verfügung gestellt hat. Die betroffene Person darf durch den Verantwortlichen nicht behindert werden, diese Daten einem anderen Verantwortlichen zur Verfügung zu stellen.

Recht auf nicht ausschließlich automatisierte Entscheidungen (Art. 22 DS-GVO)

Jede betroffene Person hat das Recht, dass Entscheidungen, die ihr gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, nicht ausschließlich automatisiert getroffen werden. So darf z. B. die Gewährung eines online beantragten Kredits nicht allein aufgrund mathematischer Algorithmen durchgeführt werden.

Recht auf Beschwerde bei einer Aufsichtsbehörde (Art. 77 DS-GVO)

Ist die betroffene Person der Auffassung, dass die Verarbeitung ihrer personenbezogenen Daten durch den Verantwortlichen gegen ihre Rechte und Freiheiten verstößt, so hat sie die Möglichkeit, sich unmittelbar an eine zuständige Aufsichtsbehörde zu wenden. Dies kann eine Aufsichtsbehörde in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes sein.

Recht, den Datenschutzbeauftragten zu konsultieren (Art. 38 DS-GVO)

Betroffene Personen können den Datenschutzbeauftragten des Verantwortlichen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zurate ziehen.

4. Datenverarbeitung durch externe Dienstleister

Dürfen andere Unternehmen mit der Verarbeitung von personenbezogenen Daten beauftragt werden?

Die DS-GVO enthält keine Regelung, dass alle innerhalb eines Unternehmens existierenden personenbezogenen Daten vom Unternehmen selbst verarbeitet werden müssen. Vielmehr ist gesetzlich vorgesehen, dass ein Unternehmen die Verarbeitung von personenbezogenen Daten in seinem Auftrag durch ein anderes Unternehmen durchführen lassen kann. Die entsprechende Regelung zur sogenannten Auftragsverarbeitung findet sich in Art. 28 DS-GVO. Dort ist festgelegt, unter welchen Rahmenbedingungen ein Auftrag an ein anderes Unternehmen, den sogenannten Auftragsverarbeiter, erteilt werden darf. Eine Bedingung ist beispielsweise, dass entsprechend den Vorgaben des Art. 28 DSGVO ein schriftlicher oder elektronischer Vertrag oder ein anderes Rechtsinstrument der Europäischen Union geschlossen werden muss. Hier wird unter anderem festlegt, in welchem Umfang und aufweiche Art und Weise die beauftragte Datenverarbeitung weisungsgebunden durch den Auftragnehmer stattfinden darf.

Werden personenbezogene Daten im Auftrag verarbeitet, sind Auftraggeber (Verantwortlicher) und Auftragnehmer (Auftragsverarbeiter) gemeinsam für die Datenverarbeitung und die Einhaltung der Regelungen der DS-GVO verantwortlich. Dabei ist der Verantwortliche verpflichtet, den Auftragnehmer so auszuwählen, dass dieser gewährleisten kann, dass der Schutz der personenbezogenen Daten ausreichend sichergestellt ist. Dem Auftragsverarbeiter ist zu untersagen, Unterauftragnehmer einzusetzen, ohne dass die vorherige schriftliche Genehmigung des Verantwortlichen vorliegt.

Was muss alles bei einer Auftragsdatenverarbeitung schriftlich festgelegt werden?

Diesen Mindestinhalt muss eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 DS-GVO haben:

- der Gegenstand und die Dauer der Verarbeitung
- die Art und der Zweck der Verarbeitung
- die Art der personenbezogenen Daten
- die Kategorien betroffener Personen
- die Pflichten und Rechte des Verantwortlichen
- Regelungen zur Beendigung des Auftragsverhältnisses wie
  - Rückgabe der Daten an den Verantwortlichen
  - die datenschutzkonforme Löschung der Daten
- die Pflichten des Auftragsverarbeiters:
  - Die Verarbeitung, insbesondere die Übermittlung, ist nur auf Basis dokumentierter Weisung durch den Verantwortlichen zulässig.
  - Informationspflicht gegenüber dem Verantwortlichen, wenn dessen Weisungen gegen Datenschutzbestimmungen verstoßen
  - Verpflichtung der beim Auftragsverarbeiter verarbeitenden Personen zur Vertraulichkeit
  - zum Schutz personenbezogener Daten getroffene technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO
  - Einhaltung der Regelungen beim Einsatz eines weiteren Auftragsverarbeiters
  - Nachweis der Einhaltung seiner Pflichten aus der Auftragsverarbeitung
  - Mitwirkungspflicht bei Überprüfungen seitens des Verantwortlichen oder eines von diesem beauftragten Prüfers
  - Unterstützung des Verantwortlichen, wenn betroffene Personen ihre Rechte wahrnehmen
  - Unterstützung des Verantwortlichen beim Vorliegen von melde- und benachrichtigungspflichtigen Sicherheitsverstößen

Dokumentation nicht vergessen!

Alle Auftragsverarbeitungsverträge sollten genau dokumentiert werden, da sie eine Übermittlung personenbezogener Daten beinhalten. Im Falle eines Lösch- oder Korrekturanspruches einer betroffenen Person müssen alle Empfänger der Daten entsprechend informiert werden.

Gelten die Bestimmungen zur Auftragsverarbeitung auch dann, wenn die Verarbeitung personenbezogener Daten nicht im Vordergrund steht?

Auch wenn bei einer an einen Dienstleister ausgelagerten Tätigkeit die Verarbeitung personenbezogener Daten nicht im Vordergrund steht, gelten unter Umständen die Vorgaben des Art. 28 DS-GVO zur Auftragsverarbeitung. Hat der Dienstleister die Möglichkeit, z. B. bei Wartungs- oder Prüfungstätigkeiten personenbezogene Daten einzusehen, fällt dies unter die Bereitstellung personenbezogener Daten und ist somit eine Verarbeitung im Sinne der DS-GVO, die unter die Regelungen der Auftragsverarbeitung fällt.

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

Beispiel:
Ihr Unternehmen nutzt eine Datenbank zur Kundenverwaltung. Ein externes Unternehmen wartet die diesbezügliche Hard- und Software, sichert die Datenbank und archiviert alte Datenbestände. Weil nicht ausgeschlossen werden kann, dass das externe Unternehmen bei der Erledigung dieser Aufgaben personenbezogene Daten zur Kenntnis nimmt, muss eine schriftliche Vereinbarung mit dem Inhalt des Art. 28 DS-GVO geschlossen werden.

Wer ist zu informieren, wenn Tätigkeiten ausgelagert werden?

Wird beabsichtigt, Tätigkeiten auszulagern oder an Dienstleister zu vergeben, bei denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, sollten Sie den betrieblichen Datenschutzbeauftragten informieren. Dieser kann prüfen, welche Maßnahmen aus datenschutzrechtlicher Sicht zu ergreifen sind, und beispielsweise bei der Ausarbeitung eines Auftragsverarbeitungsvertrags unterstützen.

Beispiel:
Datenfluss bei der Auftragsverarbeitung Ein Unternehmen möchte eine Kundenzufriedenheitsstudie durchführen. Die Befragung der Bestandskunden und die anschließende Auswertung sollen weisungsgebunden durch ein Spezialunternehmen erfolgen. Das Unternehmen erhält dann diese Ergebnisse.

5. Datentransfer im Unternehmensverbund

Was ist zu beachten, wenn Daten zwischen Unternehmen im Konzern oder im Unternehmensverbund ausgetauscht werden sollen?

Besteht beispielsweise ein Konzern oder eine Unternehmensgruppe aus verschiedenen rechtlich selbstständigen Unternehmen, dann bedeutet diese Zusammengehörigkeit nicht, dass personenbezogene Daten ohne weiteres vom einen Unternehmen an das andere Unternehmen weitergegeben werden dürfen. Die DS-GVO kennt nämlich kein sogenanntes Konzernprivileg. Im Ergebnis bedeutet das, dass die Unternehmen innerhalb eines Konzerns oder Unternehmens-verbunds datenschutzrechtlich so zu behandeln sind, als wären sie nicht miteinander verbunden: Vielmehr sind diese wie völlig unabhängige und fremde Unternehmen anzusehen.

Wann dürfen Datenzwischenverbundenen Unternehmen ausgetauscht werden?

Auch in diesem Fall gilt das sogenannte datenschutzrechtliche Erlaubnisvorbehaltsprinzip. Die Daten dürfen grundsätzlich nicht an ein anderes Konzernunternehmen weitergegeben werden. Als Erlaubnistatbestand sieht die DS-GVO in Art. 6 Abs. 1 Satz 1 lit. f das „berechtigte Interesse" des Verantwortlichen. Dabei ist laut Erwägungsgrund 48 Satz 1 DS-GVO der Datenaustausch innerhalb einer Unternehmensgruppe zu Verwaltungszwecken als berechtigtes Interesse gewertet. Die zugrundeliegende Interessenabwägung muss dokumentiert werden. Die Einwilligung als Erlaubnistatbestand muss den Anforderungen des Art. 7 DS-GVO genügen.

6. Rund um den betrieblichen Datenschutzbeauftragten

Wann braucht ein Unternehmen einen Datenschutzbeauftragten?

Die DS-GVO sieht prinzipiell Fälle vor, in denen ein Unternehmen, neben den öffentlichen Stellen, ebenfalls dazu verpflichtet ist, einen betrieblichen Datenschutzbeauftragten zu bestellen:

Ein Datenschutzbeauftragter muss bestellt werden, wenn die Kerntätigkeit des Verantwortlichen

- die umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht (z. B. Videoüberwachung),
- in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder Straftaten besteht (z.B. Gesundheitsdaten, biometrische Daten) oder aber
- die Mitgliedstaaten gemäß Art. 37 Abs. 4 weitere Pflichten zur Bestellung festlegen.

Gemäß Art. 37 Abs. 4 sind weitere Pflichten zur Bestellung festgelegt. Diese finden sich im Datenschutz-Anpassungsgesetz 2018 § 57.Benennung, Stellung und Aufgaben des Datenschutzbeauftragten

- Jeder Verantwortliche hat nach Maßgabe des Art. 37 Abs. 5 und 7 DSGVO einen Datenschutzbeauftragten zu benennen. Gerichte sind im Rahmen ihrer justiziellen Tätigkeit von der Verpflichtung zur Benennung eines Datenschutzbeauftragten ausgenommen. §§ 4 und 5 gelten im Hinblick auf die Bestimmungen dieses Hauptstücks sinngemäß.
- Für die Stellung des Datenschutzbeauftragten gilt Art. 38 DSGVO.
- Dem Datenschutzbeauftragten obliegen die in Art. 39 DSGVO genannten Aufgaben in Bezug auf die Einhaltung der Bestimmungen dieses Hauptstücks.
- Der Verantwortliche hat die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und der Datenschutzbehörde mitzuteilen.

Welche Aufgaben hat der Datenschutzbeauftragte?

Die wesentlichen Aufgaben des betrieblichen Datenschutzbeauftragten hat der Gesetzgeber in Art. 39 DS-GVO festgehalten. Danach überwacht er die Einhaltung der DS-GVO und anderer Vorschriften über den Datenschutz (Art. 39 Abs. 1 lit. b). Um dies zu gewährleisten, muss er darauf achten, dass die Datenverarbeitungsprozesse, in welchen personenbezogene Daten verarbeitet werden, ordnungsgemäß angewendet werden und somit nicht im Widerspruch zu den Vorgaben der DS-GVO stehen. Ferner zählt es zu seinen gesetzlichen Hauptaufgaben, die mit personenbezogenen Daten arbeitenden Beschäftigten des Unternehmens mit den gesetzlichen Datenschutzvorschriften vertraut zu machen. Weiterhin berät er die Mitarbeiter und die Unternehmensleitung in Fragen der ordnungsgemäßen Verarbeitung personenbezogener Daten. Ferner ist er Anlaufstelle der Aufsichtsbehörde und für betroffene Personen, die Auskunft darüber haben möchten, wie mit personenbezogenen Daten im Unternehmen umgegangen wird. Auch für Beschwerden im Umgang mit personenbezogenen Daten ist der Datenschutzbeauftragte der erste Ansprechpartner.

Muss der Datenschutzbeauftragte bei neuen Datenverarbeitungen informiert werden?

Damit auch bei neuen Datenverarbeitungsverfahren die gesetzlichen Bestimmungen zum Datenschutz eingehalten werden können, ist es erforderlich, dass der betriebliche Datenschutzbeauftragte ordnungsgemäß und frühzeitig über diese Vorhaben informiert wird.

7. Datenschutzpannen und -verstöße

Was passiert bei Datenschutzverstößen?

Wird gegen die DS-GVO verstoßen, indem unrechtmäßigerweise personenbezogene Daten verarbeitet werden, oder werden organisatorische Anforderungen der DS-GVO nicht umgesetzt, kann dies Folgen für die dafür Verantwortlichen und das Unternehmen selbst haben. Die DS-GVO nennt solche „Datenschutzpannen“, Verletzungen des Schutzes personenbezogener Daten".

In Art. 83 Abs. 4-6 sind diverse Tatbestände aufgeführt, die eine Geldbuße nach sich ziehen können. Werden beispielsweise auf einer Webseite bei der Registrierung keine datenschutzfreundlichen Voreinstellungen getroffen, droht hierfür eine Geldbuße von bis zu 10.000.000 € oder von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist (vgl. Art. 83 Abs. 4 lit. a).

Bei Verstößen gegen die Grundsätze der Verarbeitung, wie z. B. fehlende Einwilligung oder Rechtsgrundlage zur Verarbeitung, drohen hierfür Geldbußen von bis zu 20.000.000 € oder von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist (vgl. Art. 83 Abs. 5 lit. a).

Darüber hinaus kann eine „Datenschutzpanne" das Ansehen eines Unternehmens nachhaltig beeinträchtigen. Je nachdem, wie schwerwiegend die Panne ist oder das Echo in z. B. den sozialen Medien, kann es mitunter Jahre dauern, bis das einmal verlorene Vertrauen wieder zurückgewonnen ist.

Wer muss bei Verletzungen des Schutzes personenbezogener Daten informiert werden?

Diese Verletzungen müssen nach Art. 33 DS-GVO unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, der Aufsichtsbehörde gemeldet werden. Es sei denn, die Verletzung führt zu keinem Risiko für die Rechte und Freiheiten der betroffenen Person. Besteht hingegen ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen, müssen diese ebenfalls über die Verletzung und deren mögliche Folgen informiert werden. Sowohl die Meldung an die Aufsichtsbehörde als auch die an die Betroffenen unterliegen umfangreichen Mindestanforderungen bezüglich des Inhaltes. Diese werden in Art. 33 und 34 DS-GVO aufgeführt.

Kann eine Verletzung des Schutzes personenbezogener Daten auch arbeitsrechtliche Konsequenzen haben?

Kommt es durch das Handeln eines Beschäftigten zu einem solchen Datenschutzverstoß, dann kann dies auch zu arbeitsrechtlichen Konsequenzen führen. Wird der Verstoß absichtlich oder grob fahrlässig verursacht und entsteht hierdurch ein Schaden, dann kann das Unternehmen den entstandenen Schaden vom Arbeitnehmer ersetzt verlangen. Darüber hinaus kann eine Verletzung datenschutzrechtlicher Bestimmungen zu einer sogenannten arbeitsrechtlichen Abmahnung führen.

Ist dem Unternehmen die weitere Beschäftigung des Arbeitnehmers nicht mehr zuzumuten, dann kann dieses eine Kündigung aussprechen. Bei besonders schwerwiegenden Verstößen kann dies sogar fristlos erfolgen.

Kann eine betroffene Person Schadensersatz fordern?

Die DS-GVO sieht auch Schadensersatzansprüche für eine betroffene Person vor. Erleidet eine betroffene Person durch einen Verstoß gegen die DS-GVO einen materiellen oder immateriellen Schaden, hat sie einen Anspruch auf Schadensersatz gegenüber dem Verantwortlichen oder dessen Auftragsverarbeiter. Darüber hinaus können Schadensersatzansprüche nach den Regeln des Bürgerlichen Gesetzbuches (BGB) bestehen, wenn durch die Verarbeitung personenbezogener Daten das grundgesetzlich geschützte Persönlichkeitsrecht eines Betroffenen beeinträchtigt wird.

Sollen Verstöße dem Datenschutzbeauftragten gemeldet werden?

Wenn ein Mitarbeiter feststellt, dass ein anderer Mitarbeiter massiv gegen datenschutzrechtliche Vorgaben verstößt, dann sollte der Datenschutzbeauftragte umgehend informiert werden. Eine Information muss auch dann erfolgen, wenn durch das Verhalten eines Mitarbeiters die Datensicherheit für personenbezogene Daten des Unternehmens bedroht ist, z. B. durch die eigenmächtige Installation von Programmen dubioser Herkunft. Bemerken Sie, dass besonders sensible oder personenbezogene Informationen gestohlen wurden oder dem Unternehmen auf andere Weise abhandengekommen sind, informieren Sie umgehend die Geschäftsleitung und den betrieblichen Datenschutzbeauftragten. Diese werden den Vorfall unter datenschutzrechtlichen Aspekten bewerten, das weitere Vorgehen festlegen und erforderlichenfalls die Aufsichtsbehörde für den Datenschutz und die betroffenen Personen informieren.

Eine solche Information hat nichts mit „Anschwärzen" zu tun, vielmehr trägt sie dazu bei, dass im Interesse aller Datenschutz und Datensicherheit gewährleistet bleiben und empfindliche Strafen vermieden werden.

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

8. Videoüberwachung im Unternehmen

Wonach richtet sich die Zulässigkeit einer Videoüberwachung?

Die DS-GVO enthält keine expliziten Regelungen zur Rechtsgrundlage von Videoüberwachung, jedoch einige Hinweise auf deren Zulässigkeit. Daher ist die Videoüberwachung zunächst wie alle anderen Verarbeitungen personenbezogener Daten zu handhaben.

In Erwägungsgrund 91 Satz 3 wird konkret ausgeführt, dass eine Datenschutz-Folgenabschätzung für die weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen, erforderlich ist. Art. 35 DSGVO regelt dann die Durchführung der Datenschutz-Folgeabschätzung, welche nach Art. 35 Abs. 3 lit. c insbesondere für die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche erforderlich ist.

Gibt es auch außerhalb der DS-GVO Vorschriften zur Videoüberwachung?

Grundsätzlich kann einem Unternehmen auch aufgrund anderer rechtlicher Bestimmungen der Einsatz von Videokameras erlaubt oder sogar vorgeschrieben sein, wie z. B. bei der Überwachung öffentlicher Räume durch private Unternehmen. Oder denken Sie beispielsweise nur an Banken. Rechtsgrundlage für die Zulässigkeit einer Videoüberwachung können allerdings auch Vereinbarungen zwischen Arbeitgeber und Mitarbeitervertretung sein. So können beispielsweise Kollektivvereinbarungen (einschließlich Betriebsvereinbarungen) als Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Beschäftigtenkontext gelten (Art. 88 DS-GVO).

Was sind öffentlich zugängliche und nichtöffentlich zugängliche Räume?

Von einem öffentlich zugänglichen Raum spricht man immer dann, wenn ein Raum oder eine Fläche dazu bestimmt ist, von jedermann betreten zu werden.

Beispiele: Verkaufsräume, Empfangsbereich im Unternehmen, Parkplatz und Parkhaus, Warteräume und -zonen, Flughäfen. Nicht öffentlich zugänglich ist hingegen ein Raum oder eine Fläche, die nur von einer bestimmten Personengruppe betreten werden soll. Im Unternehmen sind dies in der Regel die Bereiche, in denen sich ausschließlich die Beschäftigten des Unternehmens aufhalten.

Beispiele: Produktions- und Werkshallen, Mitarbeiterparkplatz, Innenhöfe, Kantine, Großraumbüro.

Macht es einen Unterschied, ob Bilddaten gespeichert werden oder nicht?

Auch in dem Fall, dass eine Videokamera nur als „verlängertes Auge" eingesetzt wird, weil z. B. das Kamerabild der Werkseinfahrt zum Monitor beim Pförtner übertragen wird, sind die Bestimmungen der DS-GVO einzuhalten. So ist beispielsweise auch das Beobachten ohne eine Aufzeichnung der Bilddaten an den rechtlichen Zulässigkeitsvoraussetzungen zu messen.

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

Darf eine Videoüberwachung heimlich stattfinden?

Die DS-GVO trifft keine Aussage zu einem heimlichen Einsatz von Videoüberwachung und sieht auch keine Hinweispflicht für die Videoüberwachung vor.

Welche Bereiche dürfen nicht videoüberwacht werden?

Tabu sind Bereiche, bei denen eine Beobachtung oder Überwachung die Privat- und Intimsphäre des Beobachteten unzumutbar beeinträchtigen würde. Das grundgesetzlich geschützte Recht des Einzelnen auf Privatsphäre überwiegt hier immer das Interesse eines Unternehmens.

Beispiele für Tabu-Bereiche: Toiletten, Umkleiden, Waschräume, Gebetsräume, Behandlungszimmer des Betriebsarztes.

Wer prüft, ob eine Videoüberwachung zulässig ist?

Grundsätzlich ist es Sache des Unternehmens, eine Videoüberwachung so auszugestalten, dass den Anforderungen der DS-GVO entsprochen wird. Im Rahmen seiner Aufgaben kann der betriebliche Datenschutzbeauftragte bei der Datenschutz-Folgeabschätzung beratend tätig sein und eine Videoüberwachung datenschutzrechtlich bewerten. Ebenso ist dies im Rahmen seiner Überwachungsaufgaben möglich. Wichtige Prüfungspunkte dabei sind unter anderem:

- Für welchen rechtlich zulässigen Zweck wird die Videoüberwachung eingesetzt?
- Welche Bereiche werden überwacht?
- Für welchen Zeitraum werden Bilddaten gespeichert und wann werden diese wieder gelöscht?
- Ist der Einsatz von Videoüberwachung auf das erforderliche Maß beschränkt und insgesamt verhältnismäßig?

Aber auch die für das Unternehmen zuständige Aufsichtsbehörde für den Datenschutz kann die Zulässigkeit einer Videoüberwachungsmaßnahme überprüfen.

9. Datenverarbeitung im Beschäftigungsverhältnis

Gibt es spezielle Regelungen für den Umgang mit Beschäftigtendaten im Unternehmen?

„Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext [...] vorsehen", heißt in Art. 88 DS-GVO, der die Verarbeitung personenbezogener Daten im Verhältnis zwischen Unternehmen und Beschäftigtem regelt. Aber auch Vereinbarungen zwischen Unternehmen und Mitarbeitervertretung, beispielsweise Betriebsvereinbarungen, können verbindliche Regeln für das Verarbeiten personenbezogener Daten der Beschäftigten enthalten. Diese, in der DSGVO

Kollektivvereinbarung genannten Regelungen, dürfen jedoch die zugesicherten Rechte der betroffenen Personen nicht aufheben.

Wer gilt als Beschäftigter eines Unternehmens?

In Datenschutzgesetz ist festgelegt, welche Personen im Unternehmen als Beschäftigte gelten. Dies sind insbesondere

- Arbeitnehmerinnen und Arbeitnehmer,
- Auszubildende, Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis, arbeitnehmerähnliche Personen, Heimarbeiter und Gleichgestellte
- sowie Personen, deren Beschäftigungsverhältnis beendet ist.

Für die Einordnung als Beschäftigter kommt es auf die folgenden Aspekte nicht an:

- Verdienst
- Voll- oder Teilzeittätigkeit
- haupt- oder nebenberufliche Tätigkeit
- hierarchische Einordnung
- Wahrnehmung von Führungsaufgaben und Leitungsfunktionen

In welchen Fällen darf ein Unternehmen personenbezogene Daten seiner Beschäftigten verarbeiten?

Liegen in einem Mitgliedstaat der Europäischen Union keine spezifischen Regelungen gemäß Art. 88 DS-GVO vor, richtet sich die Rechtmäßigkeit der Verarbeitung allein nach der DS-GVO. Die Regelungen gelten, sofern diese nicht der DS-GVO widersprechen. Daher ist die Verarbeitung personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses zulässig, wenn dies für die Entscheidung über die Begründung, die Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist. An dieser Regelung muss beispielsweise gemessen werden, ob die Gestaltung eines Bewerberportals im Internet oder der Einsatz von Überwachungskameras auf dem Betriebsgelände datenschutzrechtlich zulässig ist. Dabei liegt der Schwerpunkt der Prüfung auf der Frage, ob die Verarbeitung zur Erreichung eines bestimmten Zwecks erforderlich ist.

Darf ein Unternehmen personenbezogene Daten verarbeiten, um Straftaten aufzudecken?

In Datenschutzgesetz ist festgelegt, dass ein Unternehmen unter bestimmten Umständen personenbezogene Daten eines Beschäftigten verarbeiten darf, um Straftaten aufzudecken. Solche Ermittlungsmaßnahmen sind zulässig, wenn

- tatsächliche Anhaltspunkte den Verdacht begründen, dass ein Beschäftigter im Beschäftigungsverhältnis eine Straftat begangen hat und

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

- das Erheben, Verarbeiten und Nutzen personenbezogener Daten für die Aufdeckung der Straftaten erforderlich sind und
- der Beschäftigte sich auf kein überwiegendes schutzwürdiges Interesse am Ausschluss der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten berufen kann.

Muss eine Mitarbeitervertretung einem Verarbeitungsverfahren zustimmen?

Für die Verarbeitung personenbezogener Daten kommen heutzutage im Unternehmen fast ausnahmslos Computer, Programme oder andere elektronische Datenverarbeitungsverfahren zum Einsatz. Gibt es im Unternehmen als Arbeitnehmervertretung beispielsweise einen Betriebsrat, bleiben diese nach § 29 Arbeitsverfassungsgesetz (ArbVG), BGBl. Nr. 22/1974 zustehenden Befugnisse unberührt. Schließlich handelt es sich bei solchen Verfahren in der Regel um technische Einrichtungen, mit denen das Unternehmen das Verhalten oder die Leistung der Arbeitnehmer überwachen könnte.

10.Datenschutz am Arbeitsplatz

Warum sollte das Clean-Desk-Prinzip eingehalten werden?

Das Thema Datenschutz geht jeden etwas an. Auch Sie können an Ihrem Arbeitsplatz dazu beitragen, dass personenbezogene Daten und vertrauliche Informationen geschützt sind und nicht in die Hände Unberechtigter gelangen. Datenschutz und Vertraulichkeit lassen sich insbesondere durch Beachtung des sogenannten Clean-Desk-Prinzips fördern.

3 Regeln des Clean-Desk-Prinzips sollten Sie besonders beherzigen

- Aufräumen
  Ordnung ist nicht nur eine Tradition aus vergangenen Zeiten, die rein praktisch der Wiederauffindbarkeit dient. Wer Ordnung hält, riskiert auch nicht, dass Daten und Informationen in die Hände Unberechtigter gelangen. Stellen Sie sich ruhig auch unter Datenschutzaspekten die Frage: „Muss das hier liegen?" Wenn nein, dann weg damit! Am besten in den Schrank oder in die Ablage.

- Wegschließen
  Jegliche Datenträger, wie etwa Notebooks, Smartphones, USB-Sticks oder Unterlagen sollten immer dann weggeschlossen sein, wenn sie nicht im Rahmen der aktuellen Arbeitsaufgabe benutzt werden müssen.

- Abschließen
  Wenn Sie länger abwesend sind, beispielsweise weil Sie zum Mittagessen gehen, in einer Besprechung sind oder Feierabend machen, sollten Sie Ihr Notebook, Mobiltelefon und Datenträger (z.B. USB-Stick oder Dokumente) nicht nur in ein sicheres Behältnis verstauen. Bitte denken Sie auch daran, dieses Behältnis, sei es Schrank oder sei es Rollcontainer, zu

verschließen und den Schlüssel abzuziehen. Lassen Sie den Schlüssel stecken, braucht es keinen Spezialisten, um an den vertraulichen Inhalt zu kommen.

Welche Mindestanforderungen sollten bei Passwörtern berücksichtigt werden?

Wenn Sie Passwörter auswählen, sollten Sie nie sogenannte Trivialpasswörter verwenden. Das sind Passwörter, die einen Bezug zum Benutzer aufweisen, wie etwa Name, Telefonnummer oder Geburtsdatum. Auch sollten nie Passwörter zum Einsatz kommen, die leicht zu erraten sind oder bei denen davon auszugehen ist, dass sie in der beabsichtigten Schreibweise auch in Wörterbüchern oder Lexika gefunden werden können. Damit ein Passwort sicher ist, sollten bei der Wahl des Passworts die folgenden Passwortanforderungen berücksichtigt werden:

idealerweise besteht das Passwort aus

- mindestens 10 Stellen.
- Es werden Ziffern, Groß- und Kleinbuchstaben sowie Sonderzeichen (z. B. §, *, #, ?) benutzt.
- Nebeneinanderliegende Tasten werden nicht verwendet (z. B. 12345 oder QWERTZ).
- Das Passwort kann nicht in Bezug zum Passwortinhaber gebracht werden (ungeeignet sind z. B. Kosename, Name des Partners, Lieblingsspeise).

Wie sollte man Passwörter aufbewahren?

Idealerweise bewahren Sie Zugangsdaten wie Benutzername und Passwort nur in Ihrem Kopf auf. Dabei ist klar, dass dies gerade bei komplexen Passwörtern schwierig ist. Bei Passwörtern bietet es sich an, dass Sie Eselsbrücken nutzen. Das geht folgendermaßen: Sie bilden Ihre Passwörter anhand von leicht zu merkenden Sprüchen oder Liedzeilen nach. So wird aus der Liedzeile „Mein Hut, der hat drei Ecken, drei Ecken hat mein Hut" das folgende Passwort MHdh333E#drei>hmH@t.

Bitte schreiben Sie Passwörter nach Möglichkeit nicht auf! Dies gilt auch dann, wenn Sie Passwörter etwa in Adressbüchern oder Telefonlisten verstecken wollen. Profis können solche versteckten Passwörter leicht ausfindig machen. Die IT-Abteilung unterstützt Sie gerne bei der Auswahl sicherer Speichermöglichkeiten, beispielsweise Software, die Ihre Passwörter verschlüsselt speichert.

Darf man Kollegen die eigenen Passwörter geben?

Passwörter gehen grundsätzlich niemanden etwas an. Das gilt auch für den noch so vertrauenswürdigen Kollegen, den Vorgesetzten oder den Mitarbeiter der IT-Abteilung. Der Grund: Wer sich unter Ihrem Benutzernamen und mit Ihrem Passwort anmeldet, gibt sich als Sie aus. Das kann böse Folgen haben. Verursacht ein Kollege unter Ihren Zugangsdaten einen Schaden, müssen Sie erst einmal beweisen, dass nicht Sie gehandelt haben. Schließlich konnten eigentlich nur Sie im Besitz der Zugangsdaten sein. Daher sollten Sie schon im Eigeninteresse nie Ihre Zugangsdaten an

Kollegen oder Bekannte geben. Haben Sie die Befürchtung, dass jemand anderer Ihr Passwort mitbekommen hat, sollten Sie Ihr Passwort unverzüglich ändern und ggf. die IT-Abteilung informieren.

Wie sollte man Unterlagen am besten entsorgen?

Unterlagen mit personenbezogenen Daten oder vertraulichen Informationen dürfen nicht einfach wie normaler Papier- oder Hausmüll entsorgt werden. Geraten personenbezogene Daten oder vertrauliche Informationen in falsche Hände, droht nicht nur dem Unternehmen erheblicher Schaden. Auch derjenige, der personenbezogenen Daten oder vertrauliche Informationen leichtfertig entsorgt, muss mit erheblichen Konsequenzen rechnen. Entsorgen Sie daher schützenswerte Unterlagen und Papierdokumente nur dann über den Papiermüll, wenn Sie sich sicher sind, dass Unbefugte die Informationen nicht mehr zur Kenntnis nehmen können. Nutzen Sie daher einen Aktenvernichter, der das Papier so weit schreddert, dass sich die Schnipsel und damit die auf dem ursprünglichen Papier enthaltenen Informationen nicht mehr zusammensetzen lassen. Steht Ihnen eine spezielle Datenschutztonne (sogenannte silberne Tonne) für die sichere und datenschutzkonforme Entsorgung von Papierdokumenten zur Verfügung, brauchen Sie diese nicht vorab in den Aktenvernichter zu geben.

Was ist bei der Entsorgung von Datenträgern zu beachten?

Sollen Datenträger wie etwa Festplatten, USB-Sticks, Daten-DVDs oder Speicherkarten entsorgt werden, muss auch hier sichergestellt sein, dass gespeicherte personenbezogene Daten und vertrauliche Informationen nicht in falsche Hände geraten. Dies kann einerseits dadurch ausgeschlossen werden, dass Datenträger mechanisch zerstört werden. Ist dies nicht möglich, muss der Datenträger datenschutzkonform gelöscht werden. Hierzu reicht es nicht aus, dass ein Datenträger mit einem Formatierungsbefehl formatiert wird. Denn die Daten bleiben auf dem Datenträger erhalten. Notwendig ist es, den Datenträger vollständig mit Nullen und Einsen zu überschreiben, am besten mehrfach. Hinsichtlich geeigneter Mittel zur Löschung von Datenträgern informiert Sie gerne die IT-Abteilung.

Wie sollte mit Besuchern und Gästen umgegangen werden?

Besucher und Gäste sollten sich nicht alleine auf dem Unternehmensgelände bewegen können. Erwarten Sie beispielsweise einen Gast oder einen Kunden, sollten Sie diesen beim Empfang abholen und nach dem Termin dort auch wieder hinbringen. Begegnen Sie nicht zum Unternehmen gehörenden Personen, die sich allein auf dem Unternehmensgelände bewegen, dürfen Sie diese ruhig ansprechen und anbieten, diese zu ihrem Ansprechpartner zu bringen. So tragen Sie dazu bei, dass Unbefugte nicht unbemerkt auf Entdeckungsreise im Unternehmen gehen.

11.Datenschutz unterwegs

Wie sollten Notebook, Datenträger und Unterlagen unterwegs aufbewahrt werden?

Wenn Sie unterwegs sind, sollten Sie Notebook, Datenträger und Unterlagen nach Möglichkeit immer so aufbewahren, dass sie den Blicken Unberechtigter entzogen sind. Das bedeutet etwa, dass ein Notebook während der Fahrt im Auto nur im Kofferraum transportiert wird. Auch im Hotel sollten Notebook, Handy, Speichermedien und vertrauliche Unterlagen sicher verstaut werden. Steht etwa ein Safe zur Verfügung, sollten Sie diesen unbedingt nutzen. Bei Tagungen und Besprechungen kann es sinnvoll sein, dass Sie Ihr Notebook mittels eines sogenannten Kabelschlosses an einem Tisch oder Heizkörper sichern. So machen Sie es potenziellen Dieben schwer und brauchen sich um Ihr Gerät in der Regel keine Sorgen machen, wenn Sie den Raum kurz für eine Kaffeepause verlassen.

Inwiefern sollte das Minimalprinzip zur Anwendung kommen?

Auf Geschäftsreise brauchen Sie in der Regel nie Ihre komplette Büroausstattung. Nehmen Sie daher nur diejenigen Gerätschaften, Speichermedien und Unterlagen mit, die Sie für Ihre Arbeit unbedingt benötigen. Wenn Sie weniger bei sich haben, erleichtern Sie dadurch nicht nur das entsprechende Gepäck. Was Sie nicht dabeihaben, kann weder gestohlen werden noch abhandenkommen.

Weshalb sollten Datenträger und Daten verschlüsselt werden?

Werden Datenträger und Daten verschlüsselt, machen Sie es Unbefugten ziemlich schwer, auf diese zuzugreifen. Möglichkeiten zur Verschlüsselung gibt es zahlreiche, etwa durch Anlegen eines verschlüsselten Dateiarchivs (sogenannte ZIP-Datei) oder durch die Nutzung von Verschlüsselungssoftware oder hardwareverschlüsselten Speichermedien. Der entscheidende Vorteil: Kommt es zu einem Diebstahl, beschränkt sich der Schaden in erster Linie auf den Materialwert der gestohlenen Sache. Weil man dank Verschlüsselung nicht auf die Daten zugreifen kann, besteht in aller Regel kein Risiko für Datenschutz und Vertraulichkeit.

Welche technischen Schutzmechanismen sind von besonderer Bedeutung?

Gerade unterwegs ist es wichtig, dass Sie vorhandene Schutzmechanismen nutzen. Deaktivieren Sie auf keinen Fall die Firewall Ihres Notebooks und schalten Sie nie die Überwachungsfunktion des Virenscanners aus. Firewall und automatische Virenerkennung sind gerade dann von Bedeutung, wenn Sie Ihren Computer mit dem Internet verbinden, etwa um E-Mails abzurufen. Sie sind aber genauso wichtig, wenn Sie Daten und Dateien von Geschäftspartnern oder Kunden erhalten, die sich auf USB-Sticks oder CDs befinden. Personenbezogene Daten auf einem mobilen Datenträger sollten immer besonders gegen unberechtigten Zugriff geschützt werden. Verschlüsselung der Daten oder des ganzen Datenträgers ist ein adäquates Mittel. Übrigens: Machen Sie es Hackern so schwer wie möglich. Wenn Sie keine Drahtlosverbindung benötigen, sollten Sie die entsprechende Funktion an Ihrem Notebook oder Ihrem Smartphone abschalten.

Was ist beim Arbeiten in Zug, Flugzeug oder in der Hotellobby zu beachten?

Bedenken Sie immer, dass Ihr Umfeld unter Umständen sehr neugierig ist und wissen will, was Sie machen. Wählen Sie nach Möglichkeit Ihren Sitzplatz so, dass Ihnen niemand über die Schulter schauen kann. Auch sogenannte Sichtschutzfolien für Notebookbildschirme, Smartphones und Smartpads sind eine datenschutzfreundliche Hilfe. Sie sorgen für eine andere Lichtbrechung, sodass Ihre Sitznachbarn nicht erkennen können, was auf Ihrem Bildschirm zu sehen ist.

Warum sollte nicht jedes verfügbare WLAN für eine Verbindung ins Internet genutzt werden?

Wenn Sie Ihr Notebook mit einem WLAN verbinden wollen, sollten Sie immer solchen WLAN-Hotspots den Vorzug geben, die von renommierten Diensteanbietern bereitgestellt werden. Bei anderen Diensteanbietern oder sogenannten wilden WLAN-Hotspots können Sie sich nie sicher sein, welche Interessen der Anbieter tatsächlich verfolgt, vielleicht wartet er – wie die Spinne im Netz - auf fette Beute. Alternativ können Sie auch Datenübertragungsdienste von Mobilfunkanbietern nutzen. Doch auch hier gilt: Wie beim WLAN ist eine Datenübertragung nur dann sicher, wenn sie verschlüsselt erfolgt. Nutzen Sie daher zur Verfügung stehende VPN-Lösungen. Die IT-Abteilung berät Sie gerne.

Was ist zu tun, wenn Computer, Datenträger oder Unterlagen gestohlen werden oder verloren gehen?

Kommt es hierzu, müssen Sie unverzüglich das Unternehmen verständigen. Informieren Sie einerseits Ihren Vorgesetzten und andererseits die IT-Abteilung. Sind personenbezogene Daten oder vertrauliche Informationen betroffen, sollten Sie zusätzlich den Datenschutzbeauftragten informieren. Diese Stellen werden die Situation bewerten und geeignete Maßnahmen in die Wege leiten. Wichtig: Wird Ihnen etwas gestohlen, sollten Sie unbedingt Strafanzeige bei der örtlichen Polizei stellen und sich die Erstattung einer Anzeige bestätigen lassen.

12.Die wichtigsten Fakten in der Übersicht

Zweck des Datenschutzes und der DS-GVO

Der Einzelne soll davor geschützt werden, dass er durch den Umgang mit seinen personenbezogenen Daten in seinen Rechten und Freiheiten, insbesondere seinem Persönlichkeitsrecht, beeinträchtigt wird.

Persönlichkeitsrecht

Das Allgemeine Persönlichkeitsrecht findet sich sowohl in der Charta der Grundrechte der Europäischen Union (Art. 7 und 8). Es räumt jedem Einzelnen das Recht auf

- Individualsphäre (Schutz des Selbstbestimmungsrechts, z.B. Recht auf informationelle Selbstbestimmung),

- Privatsphäre (Leben im häuslichen Bereich, Privatleben, z. B. Verletzung bei unverlangter E-Mail-Zusendung) und
- Intimsphäre (innere Gedanken- und Gefühlswelt)

ein.

Recht auf informationelle Selbstbestimmung

Die informationelle Selbstbestimmung ist das Recht des Einzelnen, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.

Gesetzliche Regelungen zum Datenschutz

- Datenschutz-Grundverordnung (EU DS-GVO)
- Datenschutzanpassungsgesetz des jeweiligen Mitgliedstaates
- Telekommunikationsgesetz (TKG)
- Telemediengesetz (TMG)
- Sozialgesetzbücher (SGB)
- Landesdatenschutzgesetze (LDSG)
- Regelungen der Katholischen und Evangelischen Kirche

Personenbezogene Daten

Nach Art. 4 Abs. 1 DS-GVO sind dies alle Informationen über eine identifizierte oder identifizierbare natürliche Person, die sogenannte betroffene Person. Es handelt sich dabei um Einzelangaben über persönliche oder sachliche Verhältnisse der betroffenen Person.

Verarbeitung von Daten

Zur Verarbeitung gehören das Erheben, Erfassen, Organisieren und Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen oder Verwenden, Übermitteln, die Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, Einschränken, Löschen und Vernichten von personenbezogenen Daten. Die Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten. Dies ist nur dann erlaubt, wenn es sich aus der DS-GVO, einer anderen Rechtsvorschrift oder der Einwilligung des Betroffenen ergibt.

Personenbezogene Daten im Unternehmen

- Daten der Mitarbeiter
- Daten von Bewerbern
- Daten von Kunden
- Daten von Lieferanten

Weisungsgebundenheit und Verschwiegenheit (Art. 29 OS-GVO)

Der Verantwortliche hat sicherzustellen, dass die mit der Datenverarbeitung beschäftigten Personen ausschließlich auf dessen Weisung hin und im Einklang mit den gesetzlichen Regelungen personenbezogene Daten verarbeiten. Aus Nachweisgründen wird die Verpflichtung sinnvollerweise schriftlich vorgenommen. Die Verpflichtung zur Verschwiegenheit und ordnungsgemäßen Verarbeitung personenbezogener Daten entfaltet nicht nur während Ihrer Tätigkeit für das Unternehmen Wirkung. Auch nach Ende Ihrer Beschäftigung gilt sie fort. Das bedeutet, dass Ihnen auch danach eine unberechtigte Verarbeitung von personenbezogenen Daten verboten ist.

Rechte des Betroffenen (Art. 12-23 OS-GVO)

- Das Recht auf transparente Information und Kommunikation
- das Recht auf Auskunft über personenbezogene Daten
- das Recht auf Information
- das Recht auf Berichtigung von personenbezogenen Daten
- das Recht auf Löschung (Vergessenwerden) von personenbezogenen Daten
- das Recht auf Einschränkung von personenbezogenen Daten
- das Recht auf Widerspruch
- das Recht auf Datenübertragbarkeit
- das Recht auf nicht ausschließlich automatisierte Entscheidungen
- das Recht auf Beschwerde bei einer Aufsichtsbehörde
- das Recht, den Datenschutzbeauftragten zu konsultieren

Aufgaben des Datenschutzbeauftragten (Art. 39 DS-GVO)

- Überwachung der Einhaltung der DSGVO und anderer Vorschriften über den Datenschutz
- Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme
- Schulung der Mitarbeiter im Datenschutz
- Beratung der Unternehmensleitung und der Mitarbeiter im Umgang mit personenbezogenen Daten
- Anlaufstelle für die Aufsichtsbehörden für den Datenschutz und für betroffene Personen
- Auskunftserteilung, wie mit Daten im Unternehmen umgegangen wird

Einführung neuer Datenverarbeitungsverfahren

Der betriebliche Datenschutzbeauftragte muss ordnungsgemäß und frühzeitig über diese Vorhaben informiert werden.

Einsatz von Videoüberwachung

Bei öffentlich zugänglichen Bereichen gelten die Regelungen in Art. 6 und 35 DSGVO.

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung

Verarbeitung von Beschäftigtendaten (Art. 88 DS-GVO)

Art. 88 DS-GVO erlaubt nationale Rechtsvorschriften zur Verarbeitung von personenbezogenen Beschäftigtendaten im Beschäftigungskontext. Personenbezogene Daten von Beschäftigten dürfen verarbeitet werden, wenn dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.

Unter bestimmten Bedingungen dürfen zur Ermittlung von Straftaten personenbezogene Daten der Beschäftigten erhoben, verarbeitet oder genutzt werden.

Datenschutzverstöße (Art. 83 DS-GVO)

Gegen die DS-GVO wird verstoßen, wenn unrechtmäßigerweise personenbezogene Daten verarbeitet oder wenn Anforderungen der DS-GVO nicht umgesetzt werden.

Folgen für das Unternehmen:

Je nach Tatbestand können Geldbußen von bis zu 20.000.000 € oder von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist, drohen.

„Datenschutzpannen" können zudem nachhaltig das Ansehen des Unternehmens beeinträchtigen.

Arbeitsrechtliche Konsequenzen bei Datenschutzverstößen

Wird der Verstoß absichtlich oder grob fahrlässig verursacht, kann das Unternehmen den entstandenen Schaden vom Arbeitnehmer ersetzt verlangen. Eine Verletzung datenschutzrechtlicher Bestimmungen kann zu einer sogenannten arbeitsrechtlichen Abmahnung führen. Ist dem Unternehmer die weitere Beschäftigung des Arbeitnehmers nicht mehr zuzumuten dann kann es eine Kündigung aussprechen. (Bei besonders schwerwiegenden Verstößen kann dies sogar fristlos erfolgen.)

GΞN•ICT
Gerald Langeder
Hamberg 45
A-4201 Gramastetten

M: +43(0)676-6555566
E: info@genict.com
W: www.genict.com

UID: ATU72049017
BIC: BKAUATWWXXX
IBAN: AT901200000969520246
Gerichtsstand Urfahr Umgebung