Datenschutz- und Datensicherheits-Richtlinie der d°rect Österreich

Diese Richtlinie verpflichtet die Geschäftsführung und alle Mitarbeiterinnen und Mitarbeiter zum Datenschutz und zur Datensicherheit sowie zur verantwortungs- und kostenbewussten Nutzung der informationstechnischen Einrichtungen der d°rect Österreich.

Ziel der Datenschutzrichtlinie

Die d°rect Österreich verpflichtet sich im Rahmen ihrer gesellschaftlichen Verantwortung gegenüber Kunden, Mitarbeitern und Geschäftspartnern zur Einhaltung der Datenschutzrechte. Die dafür erforderlichen Rahmenbedingungen werden über diese Datenschutzrichtlinie geschaffen.

Geltungsbereich der Datenschutzrichtlinie

Diese Datenschutzrichtlinie gilt für die d°rect Österreich.

Grundsätze für die Verarbeitung von personenbezogenen Daten.

Bei der Verarbeitung von personenbezogenen Daten handelt die d°rect Österreich stets nach den in den DSGVO verankerten Grundsätzen wie folgt:

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten werden auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet.

Zweckbindung

Personenbezogene Daten werden für festgelegte, eindeutige und legitime Zwecke erhoben und werden nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet

Datenminimierung

Personenbezogene Daten werden dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt.

Richtigkeit

Personenbezogene Daten werden sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Speicherbegrenzung

Personenbezogene Daten werden in einer Form gespeichert, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Integrität und Vertraulichkeit

Personenbezogene Daten werden in einer Weise verarbeitet, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Rechtmäßigkeit der Datenverarbeitung

Bei der Verarbeitung von personenbezogenen Daten handelt die d°rect Österreich stets im Rahmen der Rechtmäßigkeit, d.h. die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der folgenden Erlaubnistatbestände gem. Art. 6 DSGVO vorliegt:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt;

Rechte des Betroffenen

Jede betroffene Person kann ihre Rechte gegenüber der d°rect Österreich jederzeit wahrnehmen. Die entsprechende Anfrage ist umgehend durch den verantwortlichen Bereich in Abstimmung mit dem Datenschutzbeauftragten zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen. Folgende Rechte können durch den Betroffenen wahrgenommen werden:

Auskunftsrecht

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten.

Recht auf Berichtigung

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

Recht auf Löschung („Recht auf Vergessenwerden“)

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Wo ein IT-System das Löschen von Daten nicht erlaubt (z.B. im ERP-System), wird stattdessen eine Anonymisierung der Daten vorgenommen.

Recht auf Einschränkung der Verarbeitung

Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn z.B. die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt.

Recht auf Datenübertragbarkeit

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Widerspruchsrecht

Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtige ist, wenn seine schutzwürdigen Interessen aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet. Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen.

Datensicherheit

Der Schutz von personenbezogenen Daten gegen unberechtigten Zugriff, unrechtmäßiger Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung ist für die d°rect Österreich ein erklärtes Ziel.
Die d°rect Österreich hat geeignete technische und organisatorische Maßnahmen getroffen, die sicherstellen, dass die Grundsätze für die Verarbeitung von personenbezogenen Daten eingehalten werden. Dabei orientieren sich die Maßnahmen stets an dem aktuellen Stand der Technik und werden sukzessive erweitert und verbessert.
Für die Mitarbeiter gelten u.a. folgende IT-Sicherheitsrichtlinien:

1. Die Installation von Software darf ausschließlich durch Personen erfolgen, die durch die IT-Abteilung damit beauftragt wurden.
2. Mitarbeiter dürfen ohne Genehmigung der IT-Abteilung weder von zugekaufter noch von im Unternehmen selbst erstellter Software Kopien erstellen. Die Lizenzbedingungen von Softwareherstellern sind einzuhalten.
3. Der Computer des Mitarbeiters sowie mobile Datenabrufgeräte (Smartphones, Tablets etc.) sind zwingend mit einem Passwort zu schützen. Passwörter dürfen nicht schriftlich hinterlegt werden, weder als Notiz in den Büros der Mitarbeiter noch als Datei auf Computern oder Datenträgern. Passwörter dürfen unter keinen Umständen an Dritte – auch nicht an andere Mitarbeiter – weitergegeben werden.

4. Unternehmensinterne Daten dürfen nur auf den von der IT-Abteilung eingerichteten Endgeräten (PC, Notebook, Smartphone) verwendet werden. Insbesondere dürfen ohne Zustimmung der IT-Abteilung firmeninterne Datenbestände, speziell Adressbestände, Kundendaten oder Produktdaten, weder mittels E-Mail oder Fax, noch mittels anderer Datenträger (Laptop, Diskette, CD, DVD, Memory-Stick, externe Festplatte etc.) oder in ausgedruckter Form außer Haus gebracht werden.
5. Die Speicherung firmeninterner Daten darf nur in Cloud-Diensten erfolgen, die explizit von der IT-Abteilung freigegeben worden sind. Eine Nutzung privater Dienste (z.B. iCloud, Dropbox) ist untersagt.
6. Der Mitarbeiter sichert zu, dass er alle ihm im Rahmen des Vertragsverhältnisses und seiner Tätigkeit bekannt gewordene Daten, Informationen und Dokumente über die Angelegenheiten des Unternehmens, seiner Mitarbeiter, Lieferanten, Kunden und sonstigen Kontakte zeitlich unbegrenzt, insbesondere auch über die Dauer des Vertragsverhältnisses hinaus, streng vertraulich behandelt und geheim hält. Er versichert, dass er derartige Informationen Dritten nicht zugänglich machen oder sonst zum eigenen oder fremden Nutzen preisgeben wird, außer in Erfüllung seiner vertraglichen Pflichten.
7. Mitarbeiter dürfen nicht versuchen, auf Bereiche des LANs oder WANs vorzudringen, die nicht für den Mitarbeiter und sein Aufgabengebiet freigegeben oder vorgesehen sind, auch dann nicht, wenn es durch unzureichende Rechtevergabe oder technische Mängel möglich ist. Über derartige fehlerhafte Rechtevergabe oder technische Mängel ist der Vorgesetzte oder die IT-Abteilung ohne Verzug zu informieren.
8. Bei Verdacht auf Virengefahr, Datenspionage oder anderer Umstände, die die Sicherheit der Informationstechnologie des Unternehmens betreffen, ist unverzüglich ein Vorgesetzter oder die IT-Abteilung des Unternehmens zu informieren.
9. Störungen und Defekte bei informationstechnischen Einrichtungen und auftretende Fehler in der Software sind unverzüglich der IT-Abteilung zu berichten.
10. Mitarbeiter, die mit der Datensicherung beauftragt sind, haben diese Aufgaben mit besonderer Sorgfalt durchzuführen und müssen andere Vorgesetzte bzw. den EDV- Verantwortlichen unverzüglich informieren, wenn Probleme aufgetreten sind oder Gefahr im Verzug ist.

11. Jeder Mitarbeiter ist angehalten, die technischen Einrichtungen pfleglich zu behandeln und mit den informationstechnischen Ressourcen sparsam umzugehen. Das betrifft auch den Verbrauch von Speicherplatz auf den Servern und von Verbrauchmaterialien wie Druckerpapier, Druckfolien, Druckerpatronen usw.
12. Betriebsdaten müssen generell so gespeichert werden, dass bei Ausfall eines Mitarbeiters dessen Vertretung oder der Vorgesetzte auf diese Daten zugreifen kann.
13. Jeder Mitarbeiter ist angehalten, nicht mehr benötigte Dateien und E-Mails regelmäßig zu löschen und damit dazu beizutragen, dass die Datenbestände und deren Strukturen überschaubar bleiben und die Kosten der Datenhaltung und Datensicherung in vertretbaren Grenzen bleiben.
14. Verlässt ein Mitarbeiter befristet (bspw. Mutterschaft, Kur) oder unbefristet (bspw. Kündigung, Rente) das Unternehmen, so ist er /sie angehalten, nicht mehr benötigte Datenbestände und E-Mails zu löschen und die verbleibenden Datenbestände an einen Kollegen / eine Kollegin zu übergeben. Vorgesetzte sind angehalten, die ordnungsgemäße Übergabe von Datenbeständen sicherzustellen.
15. Die Privatnutzung von E-Mails ist untersagt. Auf Computern dürfen keine privaten Daten gespeichert werden. Bei Abwesenheit des Mitarbeiters ist es dem Arbeitgeber möglich, auf den Computer und den E-Mail-Account des Mitarbeiters zuzugreifen.

Datenschutzbeauftragter

Der Datenschutzbeauftragte hat eine unverzichtbare Funktion bei der Wahrung des Datenschutzes. Dazu zählen die Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften, die Beratung des Betriebes und die Schulung und Sensibilisierung der mit der Verarbeitung personenbezogener Daten betrauten Mitarbeiterinnen und Mitarbeiter. Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte zu Rate ziehen. Gemäß Art. 37 DS-GVO hat die d°rect Österreich Herrn Kevin David Schleufe als internen Datenschutzbeauftragten bestellt. Seine Kontaktdaten lauten wie folgt:

d°rect Österreich
Ing. Philipp Schweitzer BSc
Scheringgasse 2
1140 Wien
Telefon: +43 (0) 1 / 6620272 – 229
Email: datenschutz@d-rect.at

Begriffsbestimmungen

„**personenbezogene Daten**“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

„**Verarbeitung**“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

„**Einschränkung der Verarbeitung**“ ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken

„**Pseudonymisierung**“ ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

„**Verantwortlicher**“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

„**Auftragsverarbeiter**“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

„**Empfänge**r“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

„**Dritter**“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten

„**Einwilligung**“ der betroffenen Person ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

„**Verletzung des Schutzes personenbezogener Daten**“ ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

„**genetische Daten**“ sind personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

„**biometrische Daten**“ sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

„**Gesundheitsdaten**“ sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

„**Unternehmen**“ ist eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.

„**Unternehmensgruppe**“ ist eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht.