DATENSCHUTZ-RICHTLINIE ipcenter.at GmbH

Version 01.12.2025

Inhaltsverzeichnis

1 ALLGEMEINES

Zielsetzung

Die vorliegende Richtlinie stellt die verbindliche Basis für den nachhaltigen Schutz personenbezogener Daten dar. Durch Anwendung dieser Richtline soll zudem ein einheitlicher Standard geschaffen werden.

Die Verarbeitung personenbezogener Daten ist im Schulungs- und Beratungsbereich ein wesentlicher Bestandteil des Geschäftsmodells. Daher setzen sowohl Teilnehmer:innen, Kund:innen aber auch Mitarbeiter:innen einen sorgsamen Umgang mit den Daten voraus.

Sämtliche personenbezogenen Daten sind vor unbefugtem Zutritt zu schützen und entsprechend den rechtlichen Bestimmungen zu archivieren bzw. zu vernichten.

Die Einhaltung der Datenschutz-Vorgaben und die Sicherstellung der Datensicherheit tragen somit wesentlich zum nachhaltigen Unternehmenserfolg der ipcenter.at GmbH bei.

Durch die Implementierung wesentlicher Prozesse und die Einhaltung der darin festgelegten Standards werden die datenschutzrechtlichen Verpflichtungen sichergestellt.

Achtung: Mit Auftraggeber:innen bzw. Kund:innen können über diese Richtlinie hinaus zusätzliche oder strengere Regelungen vereinbart sein. Diese Pflichten, Regelungen oder Abläufe gelten über dieses Dokument hinaus und liegen in der Verantwortung der jeweiligen Geschäftsbereichsleitung (z.B. Meldepflicht von Datenschutzvorfällen an den:die Auftraggeber:in, Audits etc.).

Geltungsbereich

Die vorliegende Datenschutzrichtlinie ist für alle Mitarbeiter:innen der ipcenter.at GmbH gültig und umfasst sämtliche personenbezogenen Daten, die im Unternehmen verarbeitet werden. Darunter fallen neben Mitarbeiter:innen-Daten und Bewerber:innen-Daten auch Teilnehmer:innen-Daten im Schulungs- und Beratungskontext, sowie Kund:innen-, Geschäftspartner:innen und Expert:innen-Daten.

Zusätzlich hat sich die ipcenter.at GmbH den Branchenrichtlinien der BABE (Berufsvereinigung der Arbeitgeber:innen privater Bildungseinrichtungen) unterworfen.
Dieser „Code of Conduct“ bildet die Basis für unseren Umgang mit dem Thema Datenschutz. Die gültige Version ist auf der Infopaula abrufbar.

Die Datenschutzrichtlinie findet weiters für sämtliche Erfassungen, Erhebungen, Speicherungen und sonstige Verarbeitung personenbezogener Daten Anwendung. Bei innerbetrieblicher Weiterleitung bzw. Weitergabe sind sämtliche Aspekte der Datenschutzrichtlinie ebenso anzuwenden.

Unabhängig davon, ob die Weiterleitung bzw. Weitergabe in elektronischer oder in physischer Form erfolgt, sind die Regelungen der Datenschutzrichtline einzuhalten.

Diese Datenschutzrichtlinie ist im Einklang mit gesetzlichen Regelungen zu betrachten. Im Falle von gesetzlichen Änderungen ist jedenfalls das Gesetz maßgeblich für die Anwendung der Richtline. Sieht die gesetzliche Regelung geringere Bestimmungen als die vorliegende Datenschutzrichtline vor, ist jedenfalls die Richtlinie anzuwenden.

Verankerung im Unternehmen

Datenschutz ist ein zentrales und sehr bedeutsames Thema – aus diesem Grund obliegt die Gesamtverantwortung dafür der Geschäftsführung. Zusätzlich wurden im Unternehmen eine Datenschutzkoordination etabliert, die die Geschäftsführung bei der Einhaltung und Umsetzung der DSGVO-Vorgaben unterstützen (eine detailliertere Beschreibung dazu siehe unter Punkt 13 Zuständigkeiten).

2 Begriffe

Personenbezogene Daten

Unter dem Begriff personenbezogene Daten werden alle Daten verstanden, die einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
Im Rahmen der DSGVO wird dieser Begriff noch dahingehend erweitert, dass auch Angaben, die einen Einblick in die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität (vgl. Art. 4 Ziffer 1 DSGVO) geben, dazu zählen.

Darunter fallen u.a. folgende Daten:

- allgemeine Personendaten: Vorname, Nachname, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer etc.
- diverse Kennnummern: Sozialversicherungsnummer, Steueridentifikationsnummer, Personalausweis-, Führerschein- bzw. Reisepassnummer etc.
- Bankdaten: IBAN, BIC, Kreditinformationen, Kontostände etc.
- Online-Daten: IP-Adresse, Standortdaten etc.
- physische Merkmale: Geschlecht, Haut-, Haar- und Augenfarbe, Statur, Kleidergrößen (z.B. für Arbeitskleidung) etc.
- Besitzmerkmale: Fahrzeug- und Immobilieneigentum, Grundbucheintragungen, Kfz-Kennzeichen, Zulassungsdaten etc.
- Kund:innen-Daten: Bestellungen, Adressdaten, Bankdaten etc.
- Werturteile: Schul- und Arbeitszeugnisse etc.

Eine vollständige Aufzählung ist aufgrund der Vielzahl an zuordenbaren Datenarten nicht möglich. Ggf. ist daher vor der Datenverarbeitung Rücksprache mit dem:der zuständigen Datenschutzkoordinator:in zu halten.

Betroffene Personen

Betroffene Personen, auch „Betroffene“ genannt, sind natürliche Personen, deren Daten im Unternehmen verarbeitet werden. Die Art der Datenverarbeitung – analog oder digital – ist in diesem Fall nicht von Bedeutung. Unter dem Begriff “Verarbeitung” sind auch Datenübermittlungen, Speicherungen, das Auslesen bzw. Lesen der Daten sowie die Erhebung einzuordnen.

Besonders schutzwürdige Kategorien personenbezogener Daten (=sensible Daten)

Art. 9 DSGVO definiert einige personenbezogene Daten als besonders schutzwürdig. Die Verarbeitung dieser Daten ist generell untersagt und daher nur in bestimmten Fällen zulässig. Darunter fallen z.B. Rechte des Verantwortlichen aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsende Rechte und nur dadurch, dass der Verantwortliche den diesbezüglichen Pflichten nachkommen kann.
Die Erhebung und Verarbeitung dieser "sensiblen Daten" sind mit erhöhten Anforderungen an die Sicherheitsmaßnahmen zu deren Schutz verbunden. Erhöhte Anforderungen können die Ergreifung zusätzlicher technischer und organisatorischer Maßnahmen (TOM) sein, wie beispielsweise die ausschließlich verschlüsselte Übertragung von Daten oder ein sehr eingeschränkter Zugriff auf Daten durch wenige Personen.

In diese Kategorie fallen u.a. folgende Daten:

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- die Gewerkschaftszugehörigkeit
- genetischen Daten und biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person
- Gesundheitsdaten (Daten, die Aufschluss über körperliche oder geistige Gesundheit geben bzw. Gesundheitsdienstleistungen)
- Daten zum Sexualleben oder der sexuellen Orientierung

Datenverarbeitung

Unter Datenverarbeitung [kurz Verarbeitung] ist jeder Vorgang zu verstehen, der mit oder ohne Hilfe automatisierter Verfahren personenbezogene Daten erhebt, erfasst, organisiert, ordnet, speichert, anpasst, verändert ausliest, abfragt. Ebenso darunter fallen die Übermittlung, Verbreitung oder andere Formen der Bereitstellung sowie der Abgleich, die Verknüpfung, die Einschränkung und letztlich auch die Vernichtung oder Löschung dieser Daten.

Verletzung des Schutzes personenbezogener Daten

Eine Verletzung des Schutzes personenbezogener Daten liegt vor, wenn diese von einem sicherheitsrelevanten Ereignis betroffen sind, welches eine Missachtung der Vertraulichkeit, Verfügbarkeit oder Integrität mit sich bring und das Unternehmen für diese Daten verantwortlich ist.

3 Grundsätze und Rechtmäßigkeit der Datenverarbeitung personenbezogener Daten

Zulässigkeit der Datenverarbeitung

Generell ist vor der Verarbeitung zu prüfen, ob die Datenverarbeitung rechtlich zulässig ist. Ist dies zweifelhaft oder unklar (insbesondere bei neuen Verarbeitungen) ist der:die zuständige Datenschutz-koordinator:in zu kontaktieren.

Rechtsgrundlagen

Unterschiedliche Rechtsgrundlagen können die Basis für die Zulässigkeit der Datenverarbeitung bilden – eine Verarbeitung ist nur dann zulässig, wenn sie einem bestimmten Zweck dient und auf einer der folgenden Rechtsgrundlagen beruht:

Einwilligung

Die betroffene Person hat die Einwilligung zur Verarbeitung der personenbezogenen Daten erteilt:

- diese Einwilligung kann für einen oder mehrere bestimmte Zwecke erteilt werden;
- sie kann schriftlich, elektronisch oder mündlich erfolgen – muss jedoch unmissverständlich sein;
- eine technische Möglichkeit zur Erteilung der Einwilligung kann beispielsweise das Anklicken eines Kästchens sein – stillschweigen, bereits vorangekreuzte Kästchen oder auch Untätigkeit sind keine Einwilligungen.

Werden mehrere Zwecke der Verarbeitung zugrunde gelegt, ist für jeden Zweck eine gesonderte Einwilligung notwendig.
Sind Daten der Kategorie „sensible Daten“ zur Verarbeitung vorgesehen, ist eine ausdrückliche Einwilligung erforderlich.

Erfüllung eines Vertrages

Die Verarbeitung ist für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen.

Erfüllung einer rechtlichen Verpflichtung

Diese ist dann gegeben, wenn der Staat die Unternehmen verpflichtet, bestimmte personenbezogene Daten zu verarbeiten.
Dies umfasst die Pflicht der Anfragenbeantwortung genauso wie jene der Datenaufbewahrung.
Anwendungsfälle entstehen aus dem Arbeitsrecht, der Sozialversicherung aber auch aus dem Steuer- und Handelsrecht.

Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten

Es muss dargelegt werden können, wieso die Erhebung, Verarbeitung oder Verwendung der personenbezogenen Daten für das Unternehmen wichtig ist (die Rechte und Freiheiten von betroffenen Personen dürfen durch die berechtigten Interessen des Unternehmens allerdings nicht beeinträchtigt werden).
So kann man beispielsweise von einem berechtigten Interesse ausgehen, wenn die Verarbeitung als erwünscht angesehen wird. Hierunter fällt etwa die Zeiterfassung in einem Unternehmen, da man voraussetzen kann, dass auf Basis dieser Zeitaufzeichnung u.a. die Lohn- und Gehaltsabrechnungen vorgenommen werden.
Vielfach ist das berechtigte Interesse aber auch zugleich mit der Erfüllung rechtlicher Verpflichtungen kombinierbar. Ein Beispiel wäre die Weitergabe der Daten an ein Inkassobüro bei erfolglosen Mahnungen. Hier muss die betroffene Person damit rechnen, dass sie durch ihr Verhalten eine weitere Verarbeitung veranlasst hat.

Schutz lebenswichtiger Interessen

Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.
Eingeschlossen sind hier die körperliche Unversehrtheit sowie das Leben einer anderen Person. Dies schließt unter anderem die Verarbeitung für humanitäre Zwecke aber auch die Überwachung von Epidemien und deren Ausbreitung ein.

Wahrnehmung einer Aufgabe, die dem öffentlichen Interesse dient

Die Verarbeitung ist zur Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Hierauf können sich insbesondere Behörden oder Personen berufen, die unter das öffentliche Recht fallen.
Private Unternehmen fallen nur insoweit hinein, als sie einen Verantwortlichen mit einer derartigen Aufgabe betrauen. Dies ist aber zwingend mit einer entsprechenden Rechtsgrundlage zu verbinden, d.h. es muss eine Staatsaufgabe sein, die von dem Verantwortlichen ausgeführt wird.

Grundsätze der Datenverarbeitung

Für die Verarbeitung personenbezogener Daten gelten bestimmte Grundregeln, die einzuhalten und gegebenenfalls vom Verantwortlichen auch nachzuweisen sind; dies erfolgt unter anderem durch das Verzeichnis der Verarbeitungstätigkeiten.

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten müssen…

- auf rechtmäßige Art und Weise verarbeitet werden,
    - *Die Einwilligung zur Speicherung und Verarbeitung persönlicher Daten muss freiwillig erfolgen, sie muss spezifisch und eindeutig sein und auf entsprechender Information beruhen.*
- nach Treu und Glauben und
- in einer für die betroffene Person nachvollziehbaren Weise erfolgen.
    - *Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich & verständlich und in klarer & einfacher Sprache abgefasst sind.*
      Dies betrifft insbesondere die Information über die Identität des Verantwortlichen, die Verarbeitungszwecke sowie die Auskunft darüber, welche personenbezogenen Daten verarbeitet wurden.

Zweckbindung

Personenbezogene Daten müssen…

- für einen festgelegten, eindeutigen und legitimen Zweck erhoben werden
- und dürfen nicht in einer mit diesem Zweck nicht zu vereinbarenden Weise weiterverarbeitet werden.
    - *Die betroffene Person ist über die Verwendung der Daten bereits bei der Erhebung zu informieren und der Zweck ist ebenso im Verarbeitungsverzeichnis anzuführen. Allgemeine Formulierungen wie „künftige Forschung“, „IT-Sicherheit“ sind nicht ausreichend.*

Datenminimierung

Personenbezogene Daten müssen…

- dem Zeck entsprechen,
- sowie auf das für den Zweck der Verarbeitung notwendige Maß beschränkt sein.
    - *Dies ist dann der Fall, wenn der verfolgte Zweck nicht mit weniger Daten erreicht werden kann. Eingeschlossen sind hier sowohl die Menge der erhobenen Daten, der Umfang der Verarbeitung als auch die Dauer der Aufbewahrung und die Zugriffsberechtigungen.*
    - *Im Umkehrschluss ist sicherzustellen, dass keine Vorratsdatensammlung erfolgt. Wird beispielsweise ausschließlich per E-Mail kommuniziert, dann ist die Speicherung der Telefonnummer nicht erforderlich und darf in diesem Fall nicht als Pflichtfeld definiert werden. Werden andere als für die Verarbeitung erforderliche Daten erhoben, muss eine zusätzliche Rechtsgrundlage dafür geschaffen werden. Dies ist etwa durch eine Einwilligung möglich.*

- Datenminimierung durch Zugriffsbeschränkung
  Im Zuge der Berechtigungsvergabe ist darauf zu achten, dass Mitarbeiter:innen nur Zugriff auf jene Daten erhalten, die für die Erfüllung der Aufgaben erforderlich sind.

- Datenminimierung durch zeitliche Beschränkung
  Die Erforderlichkeit der Datenverarbeitung ist bei jedem Prozess zu definieren und gegebenenfalls auch zu evaluieren. In Verbindung mit dem Prinzip der Speicherbegrenzung gilt daher: für jeden einzelnen Verarbeitungsvorgang ist eine individuelle Speicherfrist festzulegen.

- Datenminimierung durch Pseudonymisierung und Anonymisierung
  Es gilt immer abzuwägen, ob derselbe Zweck der Verarbeitung auch erreicht werden kann, wenn personenbezogene Daten vollständig oder teilweise pseudonymisiert oder anonymisiert sind. Dies betrifft statistische Auswertung, wie etwa im Kursbereich oder auch im Bereich der Kund:innen-Analyse.

Richtigkeit

Personenbezogene Daten müssen…

- sachlich richtig
- und erforderlichenfalls auf dem neuesten Stand sein;
- außerdem sind angemessene Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf den Zweck ihrer Verarbeitung unrichtig sind, gelöscht oder berichtigt werden.

Speicherbegrenzung

Personenbezogene Daten müssen…

- in einer Form gespeichert werden,
- die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für den Zweck, für den sie verarbeitet werden, erforderlich ist.

- *Eine längere Speicherung ist nur dann zulässig, wenn ein öffentliches Interesse der Archivzwecke oder wissenschaftliche und historische Forschungs- oder statistische Zwecke gem. Art 89 Abs 1 vorliegen. Es muss aber auch in diesem Fall für die Sicherstellung geeigneter technischer und organisatorischer Maßnahmen (TOM) gesorgt werden.*

Integrität und Vertraulichkeit

Personenbezogen Daten müssen…

- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet;
- einschließlich Schutz
  - vor unbefugter oder unrechtmäßiger Verarbeitung (Vertraulichkeit),
  - vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung (Integrität)
  - durch geeignete technische und organisatorische Maßnahmen (TOM).

4 Unternehmensrelevante personenbezogene Datenverarbeitungen

Bewerber:innen-Daten

Die im Zuge des Bewerbungsprozesses notwendigen Datenverarbeitungen werden vom Supportteam „Recruiting & Karriere“ durchgeführt.

Speicherdauer: Mit Besetzung der Stelle ist der Zweck der Datenverarbeitung erfüllt. Es besteht jedoch eine gesetzliche Grundlage, die Daten dennoch für weitere 7 Monate nach der erfolgten Stellenbesetzung aufzubewahren. Zur Abwehr von etwaigen Rechtsansprüchen wegen Diskriminierung gilt eine 6-monatige Klagseinbringungsfrist. Im Anschluss daran ist ein weiterer Monat für einen etwaigen Nachlauf als angemessen zu betrachten.

Mitarbeiter:innen-Daten

Die aufgrund des Arbeitsverhältnisses notwendigen Datenverarbeitungen zur Personaladministration und für die Vorbereitung der Lohn- und Gehaltsverrechnung werden vom Supportteam „Personalbüro“ durchgeführt.

Weitere, im Rahmen der Durchführung der Lohn- und Gehaltsabrechnung notwendigen Datenverarbeitungen, werden von der eduPRO Group GmbH durchgeführt (Auftragsverarbeitungsvereinbarung vorhanden).

Speicherdauer: Mitarbeiter:innen-Daten werden basierend auf den gesetzlichen Grundlagen aufbewahrt, wobei eine Aufbewahrung dadurch auch über das Austrittsdatum hinaus gehen kann; beispielsweise muss die Ausstellung eines Dienstzeugnisses 30 Jahre ab Austritt möglich sein.

Teilnehmer:innen-Daten (Bildungsangebote)

Die Verarbeitung von Teilnehmer:innen-Daten (Bildungsangebote) erfolgt in erster Linie zum Zweck der Vertragserfüllung mit Auftraggeber:innen (v.a. AMS, ÖIF); die ipcenter.at GmbH fungiert in diesen Projekten als Auftragsverarbeiter (Auftragsverarbeitungsvereinbarungen vorhanden).

Speicherdauer: Für Teilnehmer:innen-Daten gelten die mit Auftraggeber:innen vertraglich vereinbarten Löschfristen (in der Regel 6 Monate nach Projektende).

Die ipcenter.at GmbH verarbeitet im Rahmen von Arbeitsmarktprojekten auch Daten von ÜBA-Lehrlingen, die im Auftrag von AMS und WAFF ausgebildet werden. In diesem Fall handelt die ipcenter.at GmbH einerseits als Auftragsverarbeiter des AMS und fungiert zusätzlich – in ihrer Funktion als Arbeitgeberin – auch als Verantwortlicher.

Speicherdauer: Für die Aufbewahrung der Lehrlings-Daten gelten die vertraglichen Vereinbarungen mit dem Auftraggeber AMS (in der Regel 6 Monate nach Projektende).
Lehrlings-Daten, die aufgrund des Dienstverhältnisses zu verarbeiten sind, werden entsprechend den gesetzlichen Grundlagen (Personalverrechnung) aufbewahrt.

Teilnehmer:innen-Daten (UF)

Die Verarbeitung von Teilnehmer:innen-Daten im Geschäftsbereich „Unternehmensformate“ erfolgt zum Zweck der Vertragserfüllung mit dem:der Kund:in, wie z.B. Erstellung von Teilnehmer:innen-Listen, Ausstellung von Teilnahmebestätigungen und Zertifikaten, Bereitstellung von Zugängen zu elektronischen e-learning Produkten etc.

Speicherdauer: Teilnehmer:innen-Daten werden 6 Monate nach Beendigung der jeweiligen Bildungsmaßnahme bzw. des jeweiligen Auftrages/Projektes gelöscht.

Kund:innen-, Geschäftspartner:innen und Expert:innen-Daten

Die Verarbeitung von Kund:innen- und Geschäftspartner:innen-Daten erfolgt zum Zweck der Kontaktaufnahme/Geschäftsanbahnung bzw. Geschäftsabwicklung.

Im Geschäftsbereich „International Project Unit“ erfolgt die Verarbeitung von Partner:innen-Daten (Unternehmen, Organisationen, Förderstellen) und Expert:innen-Daten auch zum Zweck der Teilnahme an Projektausschreibungen, für Projektabwicklungen und in weiterer Folge auch für die Durchführung von Projektabrechnungen.

Speicherdauer: Kund:innen- Geschäftspartner:innen- und Expert:innen-Daten werden entsprechend der rechtlichen Vorgaben bzw. lt. Vereinbarung mit dem:der Kund:in bzw. dem:der Geschäftspartner:in bzw. dem:der Expert:in gelöscht.
Detailliertere Regelungen sind den jeweiligen Bestimmungen/Verträgen/Aufträgen zu entnehmen. Die Verantwortung für die fristgerechte Löschung der Daten obliegt der jeweiligen Geschäftsbereichsleitung.

5 DATENGEHEIMNIS

Alle Mitarbeiter:innen müssen in Form einer schriftlichen Erklärung zum Datengeheimnis verpflichtet werden (Verpflichtungserklärung). Der Arbeitgeber (Verantwortlicher) ist verpflichtet dafür Sorge zu tragen, dass die Mitarbeiter:innen vertraglich an die Einhaltung des Datengeheimnisses gebunden sind.

Ziel der Verpflichtungserklärung ist es, eine datenschutzrechtliche Aufklärung und Sensibilisierung der Mitarbeiter:innen sicherzustellen und einer unbefugten/unzulässigen Datenverarbeitung entgegenzuwirken. Die Informationen zum Datenschutz im Unternehmen sind mit Beginn der Tätigkeit an den:die Mitarbeiter:in zu übergeben und durch die Verpflichtungserklärung bestätigen zu lassen. Zu verankern gilt es auch, dass die Verpflichtung zur Wahrung des Datengeheimnisses auch nach Beendigung der Tätigkeit im Unternehmen bestehen bleibt.

Mitarbeiter:innen haben die Wahrung des Datengeheimnisses durch Unterzeichnung der Datenschutz Verpflichtungserklärung zu bestätigen.

6 DATENSCHUTZINFORMATION

Die ipcenter.at GmbH übermittelt – aufgrund gesetzlicher und/oder vertraglicher Verpflichtungen – Daten an Dritte. Über den Empfängerkreis, die Speicherdauer sowie die Möglichkeit der Einwilligung zur freiwilligen Datenverarbeitung wird im Dokument „Datenschutzinformation Mitarbeiter:innen“, im Intranet (InfoPaula), auf der Website bzw. mittels persönlicher Kontaktaufnahme verwiesen.

7 DATENSICHERHEIT

Die Sicherheit der Daten ist für jedes Unternehmen von essentieller Bedeutung. Sowohl die Absicherung vor Verlust aber auch der Schutz vor unbefugtem Zugriff stehen hier im Vordergrund. Durch geeignete Maßnahmen ist zu verhindern, dass Endgeräte und Datenverarbeitungssysteme von unbefugten Personen genutzt werden können. Darüber hinaus ist nach dem „Need-to-know-Prinzip“ sicherzustellen, dass Personen nur dann und im notwendigen Ausmaß Zugriff auf personenbezogenen Daten erhalten, sofern sie diese auch für die Erfüllung ihrer Aufgaben benötigen.

Die unternehmensweiten Vorgaben sind auch Bestandteil der „Arbeitsanweisung zum Umgang mit Daten“; diese wurde – über das Intranet (InfoPaula) – an die Mitarbeiter:innen kommuniziert.

Aufbewahrung von Unterlagen / Ablagesystem

Werden personenbezogene Daten in Papierform abgelegt, so sind die Ordner entsprechend zu beschriften und mit einem entsprechendem Vernichtungsdatum zu versehen.
Als elektronischer Speicherort für personenbezogene Daten sind ausschließlich jene zulässig, die unternehmensseitig zur Verfügung gestellt werden bzw. genehmigt wurden.

Vernichtung von Unterlagen

Sämtliche Unterlagen, welche personenbezogene Daten enthalten, sind ordnungsgemäß zu entsorgen; dies gilt sowohl für die papierhafte Ablage (Verwendung von Shredder-Geräten) als auch für Datenträger (in Abstimmung bzw. nach Rücksprache mit dem EDV-Team) wie z.B. Festplatten, USB-Stick, DVD etc.

Clean Desk Policy

Im Sinne des gelebten Datenschutzes ist die Clean Desk Policy im Unternehmen zu verankern. Dadurch soll sichergestellt werden, dass Zugriffe auf Dokumente nur von berechtigten Personen/Mitarbeiter:innen erfolgen können.

Soziale Medien

Soziale Medien sind aus dem Alltag nicht mehr wegzudenken und durchaus als positiv zu werten, jedoch birgt eine „unsachgemäße“ Verwendung durchaus auch Risiken für das Unternehmen, die es einzudämmen gilt.

Um etwaige Bedrohungen oder Angriffe von Dritten möglichst auszuschließen, ist Wachsamkeit und Hausverstand bei der Erstellung oder Veröffentlichung von Fotos aus Firmen-Räumlichkeiten oberstes Gebot: Keinesfalls dürfen Zugangsdaten/Passwörter fotografiert oder gar veröffentlicht oder sonstige Informationen preisgegeben werden, die eine Verletzung des Datenschutzes oder der Datensicherheit mit sich bringen könnten. So ist beispielsweise die Preisgabe von Informationen, aus denen Routinen oder Belegungen von sensiblen Büroräumen wie Personalbüro, Buchhaltung und Geschäftsführung, hervorgehen, untersagt.

Installation von Programmen und Applikationen

Harmlos wirkende Applikationen können Schadsoftware enthalten. Aus diesem Grund sind bei sämtlichen Geräten die Installationen von Anwendungen ausschließlich durch die EDV-Administrator:innen möglich.

Kommunikation

Sowohl bei der externen als auch bei der internen Kommunikation ist darauf zu achten, dass die Vorgaben zum Schutz von personenbezogenen Daten strikt eingehalten werden.

Drucker/Scanner/Kopierer

Bei der Verwendung der Multifunktions-Geräte ist darauf zu achten, dass Ausdrucke, Scans und Kopien, welche personenbezogene Daten enthalten, nicht von unbefugten Personen eingesehen oder „mitgenommen“ werden können.

Passwörter

Der korrekte und sichere Umgang mit Passwörtern ist – im Intranet (InfoPaula) – in der Richtlinie „Umgang mit Passwörtern“ geregelt und strikt einzuhalten. Technische Vorkehrungen wurden, soweit möglich, getroffen.

8 Datenschutz bei der Telearbeit

Wird Arbeit nicht im Büro, sondern von einem anderen Ort aus geleistet, ist unbedingt auf die Einhaltung aller Vorgaben zur Wahrung von Datenschutz und Datensicherheit zu achten;
dies gilt u.a. besonders bei

- der Verwendung von Arbeitsgeräten
- der Nutzung der Software
- der Speicherung von Daten
- der Erstellung von Ausdrucken
- der Arbeit mit personenbezogenen Daten (kein Zugang für unbefugte Personen)
- der Meldung von Datenschutzvorfällen

9 Datenschutzrisiken

Besonders wichtig ist es, die unternehmensweiten Daten- und IT-Sicherheits-Vorgaben strikt einzuhalten, damit die Datenschutzsicherheit gewährleistet werden kann.

Zu den Datenschutzrisiken zählen u. a.

- Social Engeneering
  - Das Manipulieren von Personen mit dem Ziel unbefugt Zugang zu vertraulichen Unternehmensinformationen und/oder IT-System zu erhalten wird Social Engineering genannt; meist erfolgt die Kontaktaufnahme per Telefon oder E-Mail.
- Phishing
  - Unter dem Begriff „Phishing“ (von „password fishing“) versteht man Versuche, über gefälschte Websites, E-Mails oder Kurznachrichten an persönliche Daten (z.B. Daten für das Online-Banking, für Online-Shops oder Soziale Netzwerke) eines:einer Internet-Benutzer:in zu gelangen.
- Austritt von Mitarbeiter:innen
  - Ausgefolgte Gegenstände (z.B. Laptop, Diensthandy) und alle unternehmens- und kundenrelevanten Daten (Sicherheitskopien o.ä. sind zu löschen/vernichten) müssen von dem:der Mitarbeiter:in retourniert werden bzw. sind Zugriffe, Berechtigungen und E-Mail-Accounts vom EDV-Team fristgerecht zu sperren bzw. zu löschen.
- Unachtsamer Umgang mit Passwörtern
  - Passwörter dürfen niemals an andere Personen weitergegeben werden bzw. ist es untersagt, Passwörter „offen zugänglich“ zu notieren, z.B. auf einem Stehkalender am Schreibtisch, auf einem Post-it am PC oder der Rückseite der Tastatur etc., um zu verhindern, dass unbefugte Personen Zugang erhalten.

10 Verantwortungsvoller Umgang mit KI-Anwendungen

ipcenter setzt auf die Vorteile Künstlicher Intelligenz (KI) und ermöglicht seinen Mitarbeiter:innen die Nutzung von KI-Anwendungen und -Services für berufliche Zwecke. Um einen sicheren und verantwortungsvollen Umgang mit dieser Technologie zu gewährleisten und die neuen Vorgaben der seit 01.08.2024 gültigen EU-KI-Verordnung („EU – AI Act“) zu erfüllen, wurden die folgenden Richtlinien erstellt.

Was ist der „EU – AI Act“?

Der **EU AI Act** ist ein neues Gesetz der Europäischen Union, das den Einsatz von KI regelt. Er teilt KI-Systeme in verschiedene Risikoklassen ein:

- Inakzeptables Risiko: KI-Systeme, die ein inakzeptables Risiko für die Sicherheit, die Gesundheit oder die Grundrechte darstellen, sind verboten (z.B. Social Scoring).
- Hohes Risiko: KI-Systeme, die in kritischen Bereichen eingesetzt werden (z.B. Medizin, Verkehr), unterliegen strengen Anforderungen.
- Geringes Risiko: KI-Systeme mit einem geringen Risiko (z.B. Chatbots) müssen bestimmte Transparenzanforderungen erfüllen.
- Minimales Risiko: KI-Systeme mit einem minimalen Risiko (z.B. Spamfilter) unterliegen keinen besonderen Anforderungen.

ipcenter muss sicherstellen, dass die eingesetzten KI-Systeme den Anforderungen des **EU AI Acts** entsprechen.

Beispiel:
Wenn ipcenter eine KI zur Analyse von Lernerfolgskontrollen einsetzt, muss sichergestellt sein, dass diese KI keine diskriminierenden Ergebnisse liefert. Weiters ist die Einhaltung der Datenschutzbestimmungen Voraussetzung. Das bedeutet insbesondere, dass keine personenbezogenen Daten eingegeben werden dürfen.

Diese Richtlinie wird regelmäßig überprüft und an neue Entwicklungen im Bereich KI und die Vorgaben des **EU AI Acts** angepasst.

ipcenter entwickelt aktuell interne Schulungen zum Thema "KI im Unternehmen", um allen Mitarbeiter:innen einen sicheren und verantwortungsvollen Umgang mit dieser Technologie zu ermöglichen.

Nutzung von KI im Unternehmen

KI-Anwendungen können für u.a. folgende Zwecke eingesetzt werden:

- Erstellung von Schulungsunterlagen: z.B. automatisierte Erstellung von Präsentationen, Übungsaufgaben und Texten.
- Recherchen: z.B. schnelle Informationsbeschaffung, automatisierte Zusammenfassung von Artikeln.
- Analyse-Instrument: z.B. Auswertung von anonymisierten Lernerfolgskontrollen, Analyse von anonymisiertem Teilnnahmefeedback.

- Optimierung laufender Prozesse: z.B. Automatisierung von administrativen Aufgaben ohne Personenbezug.
- Unterstützung bei Vor- und Nachbereitung von Trainings: z.B. durch die Bereitstellung von individualisierten Lernmaterialien und -empfehlungen.
- Erstellung von Medieninhalten: z.B. Generierung von Bildern und Videos für Marketingmaterialien oder -beiträge.

Beispiele:

- Eine KI kann Texte für ein Handout generieren oder Bilder für eine Präsentation vorschlagen.
- Eine KI kann bei der Recherche von aktuellen Studien und Fachartikeln unterstützen.
- Eine KI kann Feedbackbögen analysieren und die Ergebnisse zusammenfassen.

Zugang und Transparenz

- Welche Tools und Systeme für betriebliche Zwecke eingesetzt werden dürfen ist in Kapitel 10 geregelt.
- KI-generierte Inhalte müssen als solche gekennzeichnet werden. Wurde ein KI-Tool bei der Erstellung einer Präsentation eingesetzt, muss dies kenntlich gemacht werden.

Vorgaben für die Kennzeichnung:

- Einen Vermerk im Impressum der Schulungsunterlagen: *"Teile dieser Unterlagen wurden unter Verwendung von KI erstellt und von unseren Trainer:innen überarbeitet."*
- Eine Fußzeile in Präsentationen: *"Mit KI-Unterstützung erstellt und von Trainer:innen validiert"*
- Bei Bildmaterial einen Quellenvermerk: *"Illustration: KI-generiert mit [Tool-Name], bearbeitet durch ipcenter [Abteilung]."*

Vertraulichkeit und Datenschutz

- Auf keinen Fall dürfen **personenbezogene Daten** (z.B. Teilnehmer:innen, Mitarbeiter:innen) in ein KI-Tool / System eingegeben, eingefügt oder verarbeitet werden, wenn es dazu keine explizite Freigabe durch die Geschäftsführung gibt.
- Abhängig von der Datenart gelten unterschiedliche Richtlinien für den Umgang mit KI-Tools (siehe Punkt 11.4)
- Bei allen Aktivitäten im Zusammenhang mit KI sind die geltenden Gesetze und Datenschutzbestimmungen, insbesondere Urheber-, Persönlichkeits- und Markenrechte, zu beachten.
- Im Zweifelsfall ist eine Anfrage an das Datenschutzteam unter **datenschutz@ipcenter.at** zu richten, die die Anfragen sachgemäß beantworten.

Was sind „vertrauliche Informationen"?

Vertrauliche Informationen umfassen alle Daten, die nicht öffentlich zugänglich sind und deren unbefugte Offenlegung dem Unternehmen oder Dritten schaden könnte. Dazu gehören insbesondere:

- Geschäftsgeheimnisse: z.B. interne Strategien, Finanzdaten, Kundenlisten.
- Personenbezogene Daten: Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (z.B. Name, Adresse, Geburtsdatum, Telefonnummer, E-Mail, Sozialversicherungsnummer, Prüfungsergebnisse von Teilnehmer:innen).

- Informationen Dritter: Daten, die ipcenter im Rahmen von Geschäftsbeziehungen anvertraut wurden und deren Weitergabe nicht gestattet ist (z.B. Daten von Kunden oder Projektpartnern).

Was sind „Verzerrungen in den Inhalten"?

KI-Systeme können aufgrund von Verzerrungen in den Trainingsdaten fehlerhafte oder diskriminierende Ergebnisse liefern. Beispiele:

- Halluzinieren: Wenn dass das Modell falsche oder erfundene Informationen generiert, die nicht auf den Trainingsdaten oder der Realität basieren. Diese Halluzinationen können sich in verschiedenen Formen äußern, z. B.:
  - **Erfundene Fakten**: Die KI gibt falsche Informationen aus, als wären sie wahr (z. B. falsche Zitate, erfundene Statistiken oder nicht existierende Personen/Orte).
  - **Fehlinterpretationen**: Die KI zieht falsche Schlussfolgerungen oder verbindet nicht zusammenhängende Konzepte.
  - **Nicht existierende Quellen**: Die KI zitiert Bücher, Artikel oder Autoren, die es gar nicht gibt.
  - **Logische Fehler**: Die KI macht unplausible oder widersprüchliche Aussagen.
- Geschlechterstereotype: Eine KI, die mit Texten trainiert wurde, in denen Frauen hauptsächlich in fürsorglichen Berufen dargestellt werden, könnte in Bewerbungsunterlagen für weibliche Jugendliche automatisch Formulierungen vorschlagen, die auf soziale Kompetenzen fokussieren, während bei männlichen Jugendlichen die Betonung auf Durchsetzungsfähigkeit und Führungsqualitäten liegt.
- Ethnische Vorurteile: Wenn eine KI zur Erstellung von Schulungsunterlagen mit Daten verwendet wird, die hauptsächlich Personen einer bestimmten ethnischen Gruppe zeigen, könnte sie Bilder oder Beispiele generieren, die andere ethnische Gruppen unterrepräsentieren oder stereotyp darstellen.
- Soziale Diskriminierung: Eine KI, die beispielsweise zur Analyse von anonymisierten Bewerbungsunterlagen eingesetzt wird, könnte aufgrund von Verzerrungen in den Trainingsdaten Jugendliche aus sozial benachteiligten Verhältnissen benachteiligen, indem sie deren Qualifikationen und Potenziale unterschätzt.

Verwendete KI-Systeme und rechtliche Einordnung

Die von ipcenter genutzten generativen KI-Systeme (siehe auch Arbeitsanweisung zum Umgang mit Daten – Kapitel 10) fallen in die Kategorie der allgemein einsetzbaren KI-Systeme (General Purpose AI Systems – GPAIS). Diese Systeme können anhand weniger Eingaben komplette Texte oder Bilder erstellen und sind vielseitig einsetzbar. Gemäß der EU-KI-Verordnung (gültig ab 1. August 2024) müssen für diese Systeme gesetzliche Anforderungen beachtet werden.

- **Transparenz:** Nutzer:innen müssen darüber informiert werden, dass sie mit einem KI-System interagieren.
- **Kennzeichnungspflicht:** KI-generierte Inhalte müssen als solche gekennzeichnet werden.

- **Datenschutz:** Die Nutzung von GPAIS muss den geltenden Datenschutzbestimmungen entsprechen.

11 Dokumentationspflicht

Verzeichnis der Verarbeitungstätigkeiten (Verarbeitungsverzeichnis)

In Art. 5 Abs. 2 DSGVO ist geregelt, dass der Verantwortliche für die in Art. 5 Abs. 1 DSGVO genannten Pflichten verantwortlich ist und für deren Einhaltung einen Nachweis erbringen muss. Darunter ist eine Auskunftspflicht zu verstehen, die im Fall einer Nachfrage zu erfolgen hat. Um der Nachweis- und Auskunftspflicht Rechnung zu tragen ist schriftlich das Verzeichnis der Verarbeitungstätigkeiten zu führen.

Mindestbestandteile des Verarbeitungsverzeichnisses sind:

- Name und Kontaktdaten des Verantwortlichen
- Daten eines mit ihm gemeinsamen Verantwortlichen
- Daten seines Vertreters
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen sowie der personenbezogenen Daten
- Kategorien von Empfänger:innen (inkl. Empfänger:innen in Drittstaaten sowie internationalen Organisationen)

Zusätzlich sollten in dem Verarbeitungsverzeichnis angeführt werden:

- Löschfristen
- Beschreibung technischer und organisatorischer Maßnahmen (TOM)

Das Verarbeitungsverzeichnis ist immer aktuell zu halten. Hierzu ist vor der Einführung von neuen Prozessen oder Verfahren, welche die Verarbeitung personenbezogener Daten beinhalten, die Informationen zu dieser geplanten Verarbeitung zur Verfügung zu stellen und inhaltlich durch den:die zuständige Datenschutzkoordinator:in zu prüfen bzw. freizugeben.

Auftragsverarbeiter müssen ebenso ein schriftliches Verzeichnis führen, in dem alle Datenkategorien betreffend der im Auftrag des Verantwortlichen durchgeführten Tätigkeiten enthalten sind. Auch dieses Verzeichnis ist auf Anfrage der Datenschutzbehörde zur Verfügung zu stellen.

Einführung neuer Systeme der Datenverarbeitung

Sollen neue Systeme zur Verarbeitung von Daten – insbesondere von personenbezogenen Daten – im Unternehmen eingeführt werden, so ist dieses Vorhaben im Vorfeld dem:der zuständigen Datenschutzkoordinator:in bekannt zu geben und abzustimmen.

Sämtliche datenschutzrechtliche Aspekte sind durch die durchführende(n) Person(en)/Abteilung jedoch von Beginn an in die Spezifikation mitaufzunehmen und in der Architektur der Datenverarbeitung zu berücksichtigen.

12 Auftragsverarbeitung (AV)

Begriff

Eine Auftragsverarbeitung liegt vor, wenn ein Unternehmen (Auftraggeber:in) eine:n externe:n Dienstleister:in (Auftragnehmer:in) mit personenbezogener Datenverarbeitung beauftragt, wobei diese Verarbeitung weisungsgebunden erfolgt. Der:Die Auftraggeber:in ist für die ordnungsgemäße Datenverarbeitung weiterhin verantwortlich und der:die Auftragnehmer:in ist unterstützend tätig. Dies trifft auch auf Wartungs- und Prüfverträge zu, sobald ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Gängige Beispiele aus der Praxis:

- Beauftragungen durch das Arbeitsmarktservice (AMS)
- Beauftragungen durch den Österreichischen Integrationsfonds (ÖIF)
- Beauftragungen durch den Wiener Arbeitnehmer:innen-Förderungsfonds (WAFF)
- Auslagerung der Lohn- und Gehaltsabrechnung an externe Dienstleister:innen (ausgenommen sind Steuerberater und Wirtschaftsprüfer, diese agieren als Verantwortlicher)
- Call Center wird für Datenerhebungen (Kund:innen) des:der Auftraggeber:in eingesetzt
- Beauftragung von externen Programmierer:innen mit der Installation, Pflege, Überprüfung und Korrektur von Software
- Beauftragung von externen IT-Dienstleister:innen für die Überprüfung, Reparatur und den Austausch von Hardware
- Beauftragung von externen Dienstleister:innen mit der Aktenvernichtung

Auftragsverarbeitungsvereinbarung

Vor Beginn der Tätigkeit müssen die Vertragspartner:innen eine Vereinbarung zur Auftragsverarbeitung gem. Art 28 DSGVO abschließen. Der:Die Auftraggeber:in ist als (Haupt)Verantwortlicher für die Einhaltung des Datenschutzes verantwortlich und muss in regelmäßigen Abständen die Einhaltung des Datenschutzes kontrollieren.

Geregelt werden müssen:

- Gegenstand und Dauer des Auftrags,
- Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung / Nutzung von Daten,
- Art der Daten und der Kreis der Betroffenen,
- die nach Art. 32 DSGVO zu treffenden technischen und organisatorischen Maßnahmen,
- Berichtigung, Löschung und Sperrung von Daten
- bestehende Pflichten des:der Auftragnehmer:in, insbesondere die von ihm:ihr vorzunehmenden Kontrollen,
- etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- Kontrollrechte des:der Auftraggeber:in und entsprechende Duldungs- und Mitwirkungspflichten des:der Auftragnehmer:in,
- mitzuteilende Verstöße des:der Auftragnehmer:in oder der bei ihm:ihr beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
- Umfang der Weisungsbefugnisse, die sich der:die Auftraggeber:in gegenüber dem:der Auftragnehmer:in vorbehält,

- Rückgabe überlassener Datenträger und die Löschung bei dem:der Auftragnehmer:in gespeicherter Daten nach Beendigung des Auftrags.

13 Betroffenenrechte

Personen, die von einer Datenanwendung betroffen sind, haben gegenüber dem Verantwortlichen bestimmte Rechte.

Recht auf Information / Informationspflicht

Betroffene müssen über die Details der Datenverarbeitung und ihre Rechte informiert werden (wer / was / wann / wo / wie / wieso).

Recht auf Auskunft

Nur der Verantwortliche hat die Auskunft an die betroffene Person (Auskunftswerber:in) zu erteilen. Der:Die Auskunftswerber:in muss die Identität nachweisen, wenn der Verantwortliche berechtigte Zweifel hat.

Wird ein Auskunftsbegehren an einen Auftragsverarbeiter gestellt, so muss darauf hingewiesen werden, dass der Verantwortliche Auskunft zu erteilen hat. Das Ersuchen muss nicht weitergeleitet werden, im Sinne der Unterstützungspflicht kann es aber dennoch zielführend sein.

Der Verantwortliche muss unverzüglich antworten und die Auskunft binnen eines Monats erteilen. Sollte aufgrund der Komplexität und der Anzahl vorliegender Ansuchen die Bearbeitung innerhalb eines Monats nicht möglich sein, kann die Frist um weitere zwei Monate gestreckt werden. Hierzu ist es erforderlich die betroffene Person binnen des ersten Monats unter Angabe der Gründe darüber in Kenntnis zu setzen.

Werden durch den Verantwortlichen große Mengen an Informationen über den:die Auskunftswerber:in verarbeitet, kann um eine Präzisierung der angefragten Informationen bzw. Verarbeitungsvorgänge ersucht werden. Wird dies durch den:die Auskunftswerber:in abgelehnt, muss der Verantwortliche eine über alle Datenbestände reichende Auskunft erteilen.

Die Auskunft hat in der Regel schriftlich zu erfolgen; wurde der Antrag elektronisch eingebracht (z.B. per E-Mail) so kann dieser auch auf diese Weise übermittelt werden. Ebenso ist auf Wunsch des:der Auskunftswerber:in die postalische Übermittlung in Form einer Kopie der Daten zulässig. Mündliche Auskünfte können nur dann erteilt werden, wenn an der Identität des:der Auskunftswerber:in keinerlei Zweifel bestehen.

Recht auf Berichtigung

Jede Person kann die unverzügliche Berichtigung unrichtig oder unvollständig verarbeiteter Daten verlangen.

Unrichtige Daten, d.h. Daten, die inhaltlich unwahr sind, können beispielsweise geänderte Namen oder Adressdaten sein. In diesem Zusammenhang ist es unerheblich, ob die Daten bereits bei der Erfassung unrichtig waren, oder zu einem späteren Zeitpunkt unrichtig geworden sind.

Der Anspruch bezieht sich immer auf Tatsachenangaben und nicht auf Meinungen oder Werturteile.

Wird von der betroffenen Person der Anspruch erhoben, ist diesem unverzüglich nachzukommen. Es ist jedoch auf eine Identifikation der Betroffenen sowie die Dokumentation der Berichtigung zu achten.

Recht auf Löschung / Vergessenwerden

Die Löschung der Daten hat zu erfolgen, sobald die Rechtsgrundlage zur Datenverarbeitung nicht mehr gegeben ist.

Dies kann u.a. der Fall sein, wenn

- der Verarbeitungszweck weggefallen ist
- der Betroffene die Einwilligung widerrufen hat
- gem. Art 21 DSGVO wirksam widerrufen wurde
- die Datenverarbeitung unrechtmäßig erfolgt ist
- eine rechtliche Verpflichtung zur Löschung (z.B. Gesetz, Urteil, Bescheid) gegeben ist

Eine Verpflichtung zur Löschung durch den Verantwortlichen ist weiters gegeben, wenn eine unrechtmäßige Datenverarbeitung erfolgt ist.

Recht auf Vergessenwerden

Dieses Recht kommt dann zur Anwendung, wenn personenbezogene Daten durch den Verantwortlichen öffentlich gemacht wurden. Darunter fallen beispielsweise Verlinkungen zu Suchergebnissen in Suchmaschinen. Der Verantwortliche muss in diesen Fällen auch alle Möglichkeiten ausschöpfen, die Löschung auch bei Dritten zu bewirken.

Recht auf Einschränkung

Eine Einschränkung der Verarbeitung kann durch die betroffene Person verlangt werden, wenn

- die Richtigkeit der Daten bestritten wird
- die Datenverarbeitung unrechtmäßig erfolgt ist aber keine Löschung beantragt wird
- für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen eine fortgesetzte Speicherung verlangt wird
- durch die betroffene Person gem. Art 21 Abs 1 DSGVO ein Widerspruch zur Verarbeitung der Daten eingebracht wurde, es jedoch noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Wird das Recht auf Einschränkung der Verarbeitung geltend gemacht, hat der Verantwortliche dafür Sorge zu tragen, dass die Daten nicht mehr (weiter)verarbeitet werden. Weiters hat der Verantwortliche auch alle EmpfängerInnen (z.B. Auftragsverarbeiter) darüber in Kenntnis zu setzen.

Recht auf Datenübertragbarkeit

Erfolgt die Datenverarbeitung auf Grundlage einer Einwilligung und durch Einsatz automatisierter Verfahren, kann eine Datenübertragung erfolgen (ausgenommen sind daher Dokumente in Papierform).

Die betroffene Person hat das Recht, diese an einen anderen Verantwortlichen übermitteln zu lassen und ist darüber auch zu informieren. Dies sind Daten, die aktiv zur Verfügung gestellt wurden (z.B. Eingabe in ein Kontaktformular, Fotos auf Social Media Plattformen aber auch Aktivitätsprotokolle, Websites-Suchverläufe o.ä.). Die Übermittlung hat je nach Umfang per E-Mail, Download oder auch mittels Datenträger mit entsprechenden Datensicherheitsmaßnahmen (Verschlüsslung) zu erfolgen.

Recht auf Widerspruch / Widerruf

Erfolgte das Recht zur Verarbeitung der Daten auf Basis einer Einwilligungserklärung besteht die Möglichkeit diese jederzeit zu widerrufen. Dieser Widerruf hat mit sofortiger Wirkung seine Gültigkeit und hat auf den bestehenden Vertrag keinen Einfluss, so lange dieser durch den Widerruf weiterhin erfüllbar ist.

Konkret bedeutet das, dass der Widerruf vielfach Teilbereiche eines Vertrages betrifft, nicht aber den gesamten Vertrag und dieser somit weiterhin zu erfüllen ist.

Anfragen von Personen zur Ausübung der Betroffenenrechte sind ausnahmslos an das Datenschutzteam datenschutz@ipcenter.at weiterzuleiten, die diese Begehren sachgemäß behandeln.

14 ZUSTÄNDIGKEITEN

Datenschutzorganisation im Unternehmen

Die im Unternehmen mit der jeweiligen Datenverarbeitung betrauten Personen sind für die Einhaltung der Vorgaben dieser Richtlinie verantwortlich. Die Führungskräfte stellen sicher, dass die Richtlinie den ihnen zugeordneten Mitarbeiter:innen bekannt ist.

Bei der ipcenter.at GmbH ist eine **Datenschutzkoordination** *(Monika Kovacs)* eingerichtet. Diese stellt insgesamt die Einhaltung der Datenschutzvorgaben und der CoC bei ipcenter sicher und berichtet der Geschäftsführung.

Allgemeines Aufgabengebiet der Datenschutzkoordination:

- Formale Struktur und methodische Herangehensweise des Datenschutzes
- Koordination der datenschutzrechtlichen Aktivitäten im Unternehmen
- Überwachung der Einhaltung der gesetzlichen Bestimmungen des Datenschutzes
- Prüfung der Einhaltung der Datenschutzrichtline und der CoC
- Allgemeine Datenschutz-Schulung und Sensibilisierung der Mitarbeiter:innen

Abteilungsspezifisches Aufgabengebiet der Datenschutzkoordination:

- Beratung, Unterstützung und Kontrolle in Datenschutzfragen des (Geschäfts)Bereichs
- Datenschutzkonforme Prozessentwicklung und -verantwortung in den (Geschäfts)Bereichen
- prozessbezogene Schulung und Sensibilisierung der Teams
- Dokumentation von Datenschutzvorfällen und Interventions-Entscheidungen
- Protokollierung von Datenschutz-Entscheidungen im (Geschäfts)Bereich
- kontinuierliches Datenschutzmanagement als Abteilungsprozess

Erreichbarkeit Datenschutzkoordinatorin: datenschutz@ipcenter.at

Prozess bei Verstößen

Erlangen Mitarbeiter:innen Kenntnis von einem Verstoß in Zusammenhang mit personenbezogenen Daten, gegen diese Datenschutzrichtlinie oder gesetzliche Bestimmungen, ist umgehend per E-Mail

das Datenschutzteam datenschutz@ipcenter.at zu verständigen und konkret zu informieren (Dokumentation in der Excel-Liste „Meldung DS-Vorfälle“).
Ob eine Informations-/Meldepflicht gegenüber der Aufsichtsbehörde vorliegt wird in enger Abstimmung mit der Geschäftsführung geprüft und entschieden.

Bei Fällen, in denen die ipcenter.at GmbH als Auftragsverarbeiter fungiert, entscheidet die verantwortliche Geschäftsbereichslungsleitung, ob und in welcher Form der:die Auftraggeber:in zu verständigen ist. Beispielsweise betrifft dies Vorfälle in Projekten, die im Auftrag von AMS oder ÖIF durchgeführt werden.

Sollte eine Kontaktaufnahme mit der Datenschutzbehörde erforderlich sein, erfolgt diese ausnahmslos durch die Geschäftsführung.

Datenschutzvorfall / Data Breach

Ein Datenschutzvorfall ist grundsätzlich jedes Ereignis, in dem die Vertraulichkeit, Verfügbarkeit oder Integrität personenbezogener Daten verletzt wurde.

Die DSGVO definiert eine „Verletzung des Schutzes personenbezogener Daten“ (Data Breach) als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Interne Meldung / Dokumentation

Datenschutzvorfälle, dazu zählen beispielsweise:

- Versand einer E-Mail an einen:eine falsche:n Empfänger:in
- Versand einer E-Mail an „viele“ Empfänger:innen im Feld „cc“ anstatt „bcc“ – E-Mail-Adressen für alle Empfänger:innen ersichtlich
- Postsendungen wurden versehentlich geöffnet oder sind verloren gegangen,
- Verlust oder Diebstahl von Speichermedien (z.B. USB-Stick) oder Unterlagen – unbefugte Personen können Daten einsehen/lesen
- Verlust oder Diebstahl von Mobilgeräten (z.B. Diensthandy oder Laptop)
- Datenpannen/Datenlecks (z.B. Softwarefehler, Angriffe auf das IT-System durch Hacking)
- Stromausfall – dadurch zwischenzeitlich kein Zugriff auf das System/die Datenbank
- Versehentliche Änderungen oder auch die unbeabsichtigte Löschung von personenbezogenen Daten etc.

sind **unverzüglich** nach Bekanntwerden bzw. nach Verursachung per E-Mail an das Datenschutzteam datenschutz@ipcenter.at zu melden, da Fristen für Weitermeldungen (z.B. an die Aufsichtsbehörde) strikt eingehalten werden müssen (eine Nichteinhaltung kann für das Unternehmen schwerwiegende Folgen, einschließlich behördlicher Verfahren mit erheblichen Strafen nach sich ziehen).

Daher ist unbedingt auch im Zweifelsfall – handelt es sich schon um einen Datenschutzvorfall oder doch nicht – das Datenschutzteam zu kontaktieren: „Es ist besser einmal zu oft als nicht zu melden“.

Die interne Meldung hat folgende Informationen zu enthalten:

- Datum des Vorfalls,
- in welcher Abteilung hat sich der Vorfall ereignet,
- eine detaillierte Beschreibung des Vorfalls,
- welche Datenkategorie(n), z.B. Vor- und Nachname, E-Mail-Adresse, Lebenslaufdaten etc. sind betroffen,
- welche Personenkategorie(n), z.B. Teilnehmer:innen, Trainer:innen, Mitarbeiter:innen, Kund:innen etc. (wenn möglich, eine Anzahl der betroffenen Personen anführen) sind betroffen.

Der Vorfall wird in der Excel-Liste „Meldung DS-Vorfälle" dokumentiert und es wird eine Risikoabwägung durchgeführt. Im Anlassfall werden umgehend informiert:

- Leitung des/der betroffenen Geschäftsbereichs/Abteilung
- EDV-Team (wenn es der Vorfall erfordert, schnellstmögliche Einleitung von Sicherheitsvorkehrungen)
- die Geschäftsführung (trifft abschließend die Entscheidung, ob der Vorfall an die Aufsichtsbehörde gemeldet werden muss).

Die interne Meldung / Dokumentation aller Datenschutzvorfälle gewährleistet ein DSGVO-konformes Vorgehen und stellt sicher, dass anhand einer Risikoabwägung festgestellt wird, ob bzw. welche Maßnahmen zu ergreifen sind und ob eine Meldung an die Aufsichtsbehörde bzw. eine Benachrichtigung der betroffenen Person(en) erfolgen muss.

Meldung an die Aufsichtsbehörde (Datenschutzbehörde/DSB)

Diese muss **unverzüglich und möglichst binnen 72 Stunden** nachdem dem Verantwortlichen diese Verletzung bekannt wurde, erfolgen. Erfolgt die Meldung erst nach Ablauf von 72 Stunden, so ist diese Verzögerung zu begründen.

Die Meldung hat zumindest folgende Informationen zu enthalten:

- Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten (wenn möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der personenbezogenen Datensätze),
- den Namen und die Kontaktdaten des Datenschutzbeauftragten (falls vorhanden) oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,
- eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Verantwortliche muss alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten (Auswirkungen, ergriffene Abhilfemaßnahmen) dokumentieren. Diese Dokumentation dient der Aufsichtsbehörde zur Überprüfung der korrekten Einhaltung der Meldepflicht.

Sollte eine Kontaktaufnahme mit der Datenschutzbehörde erforderlich sein, erfolgt diese ausnahmslos durch die Geschäftsführung.

Benachrichtigung der betroffenen Person(en)

Die betroffene(n) Person(en) ist/sind im Falle eines voraussichtlich hohen Risikos unverzüglich von der Datenschutzverletzung zu benachrichtigen.

Diese Benachrichtigung muss zumindest Folgendes beinhalten:

- Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten in klarer und einfacher Sprache,
- den Namen und die Kontaktdaten des Datenschutzbeauftragten (falls vorhanden) oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung,
- eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Eine Benachrichtigung der betroffenen Person ist **nicht** erforderlich, wenn

- auf die von der Verletzung betroffenen personenbezogenen Daten geeignete technische und organisatorische Sicherheitsvorkehrungen angewandt wurden (insbesondere, wenn dadurch unbefugte Personen keinen Zugang zu diesen Daten haben, etwa durch Verschlüsselung),
- der Verantwortliche durch nachträgliche Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person aller Wahrscheinlichkeit nach nicht mehr besteht, oder
- die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall muss jedoch eine öffentliche Bekanntmachung erfolgen, oder eine ähnliche Maßnahme ergriffen werden, damit die betroffenen Personen vergleichbar wirksam informiert werden.

Eine Kontaktaufnahme mit der/den betroffenen Person(en) erfolgt nach Abstimmung mit der Datenschutzkoordination. Sind Teilnehmer:innen aus Arbeitsmarktprojekten betroffen, obliegt die finale Entscheidung über eine Verständigung der betroffenen Person(en) der zuständigen Geschäftsbereichsleitung; in allen anderen Fällen der Geschäftsführung.

15 Schlussbestimmung

Diese Datenschutzrichtlinie ist allen Mitarbeiter:innen des Unternehmens in geeigneter Form bekannt zu machen.

Änderungen und Weiterentwicklungen werden kontinuierlich vorgenommen und entsprechend in diese Richtlinie eingearbeitet. Über Aktualisierungen werden die Mitarbeiter:innen über das Intranet (InfoPaula) in Kenntnis gesetzt.