INTERNE DATENSCHUTZRICHTLINIE

der

Dimedio GmbH

Stand: 1. September 2023, Version 1.0

1. Einleitung

Diese Richtlinie ist die verbindliche Grundlage für einen rechtskonformen und nachhaltigen Datenschutz durch die Dimedio GmbH (nachfolgend "Dimedio", "Unternehmen" oder "Verantwortliche" genannt).

Mit dieser Richtlinie soll gewährleistet werden, dass die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere ihr Recht auf Schutz personenbezogener Daten, gewahrt und geschützt werden.

Die Richtlinie ist für Sie als Mitarbeitende(r) verbindlich, wann immer Sie Personendaten von Dimedio verarbeiten, unabhängig davon, ob dies elektronisch oder in Papierform erfolgt. Die Bestimmungen dieser Richtlinie bilden Bestandteil der vertraglichen Pflichten des Arbeitsvertrages mit dem Mitarbeitenden, welche stets beachtet werden müssen.

Dimedio behält sich vor, besondere Richtlinien zu erlassen, die diese Richtlinie weiter ausführen oder ergänzen, sofern dies als angemessen erachtet wird oder dies notwendig ist, um geltendes Recht einzuhalten. Die Richtline ergänzt das anwendbare Datenschutzrecht, welches vorgeht, wenn es eine Abweichung von dieser Datenschutzrichtlinie erfordert oder weitergehende Anforderungen stellt. Insbesondere wenn Personendaten ausserhalb der Schweiz bearbeitet werden oder Personen ausserhalb der Schweiz betreffen, muss jeweils geprüft werden, ob Gesetze mit strengeren Vorschriften anwendbar sind, welche dieser Richtlinie vorgehen.

Wenn Sie mit Bezug auf die Bearbeitung von Personendaten unsicher sind oder Fragen haben, ist die Anlaufstelle für Datenschutz andreas.stutz@dimedio.ch (nachfolgend "Anlaufstelle für Datenschutz" genannt) zu kontaktieren.

2. Wann liegt eine relevante Verarbeitung von Personendaten vor

Als "Personendaten" gelten alle Informationen über Personen, welche namentlich genannt werden oder welche aus anderen Gründen einer bestimmten Person zugeordnet werden können. Das können beispielsweise Angaben über andere Mitarbeitende, Kunden oder Lieferanten sein, wie bspw. Name, Geschlecht, Foto, Geburtstag, Email-Adresse, Bankkonto oder Sozialversicherungsnummer.

Als "Verarbeiten oder Bearbeiten" gilt jeder Umgang mit Personendaten, wie beispielsweise das Beschaffen, Aufbewahren, Speichern, Umarbeiten, Weitergeben oder Vernichten von Personendaten. Beispiel: Eine Verarbeitung von Personendaten liegt vor, wenn Sie Angaben über Mitarbeitende oder über Kunden im IT-System erfassen.

Personendaten können auch "besonders schützenswerte Personendaten" enthalten, wie etwa Angaben zur Gesundheit, Religionsangehörigkeit oder Rassenzugehörigkeit, politische Meinungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Sensible Daten), Personendaten betreffend Straftaten und/oder Verurteilungen oder Personendaten von Kindern unter sechzehn Jahren. Wann immer wir besonders schützenswerte Personendaten verarbeiten, sind die strengeren Vorgaben gemäss nachfolgendem Artikel 3.2. einzuhalten.

3. Prinzipien für die Verarbeitung von Personendaten

Alle Mitarbeitenden von Dimedio bei der Verarbeitung von Personendaten folgende Datenschutzprinzipien einhalten:

Rechtmässigkeit	Wir erheben Personendaten nur, wenn wir eine rechtliche Grundlage dafür haben.
Besonders schützenswerte Personendaten und Persönlichkeitsprofile	Wir beachten weitere strengere Vorgaben, wenn wir besonders schützenswerte Personendaten verarbeiten oder Persönlichkeitsprofile erstellen.
Fairness und Transparenz	Wir verarbeiten Personendaten in transparenter Weise und informieren die betroffene Person vorgängig, in umfassender und leicht verständlicher Weise über die Datenverarbeitung, damit die betroffene Person diese nachvollziehen kann.
Zweckbindung	Wir erheben Personendaten ausschliesslich für festgelegte, eindeutige und rechtmässige Zwecke.
Datenminimierung	Wir erheben nur die Personendaten, die dem Zweck nach angemessen sind und nur diejenigen, die für die Erreichung des Zweckes unbedingt notwendig sind.
Richtigkeit	Wir stellen sicher, dass die Personendaten jederzeit sachlich richtig und aktuell sind.
Speicherbegrenzung	Wir behalten und verarbeiten Personendaten nur so lange, als dies für die Erreichung des Zwecks, für die sie erhoben wurden, notwendig ist, es sei denn, ein legitimer Grund für eine längere Aufbewahrung liegt vor.
Vertraulichkeit und Integrität	Wir behandeln Personendaten vertraulich und verarbeiten diese in einer Weise, die eine angemessene Sicherheit, Schutz und Integrität der Personendaten gewährleistet.
Übermittlung oder Auslagerung an Auftragsverarbeiter	Wenn wir eine Datenverarbeitung an einen Auftragsverarbeiter auslagern (outsourcen) oder übertragen, prüfen wir diesen sorgfältig auf hinreichende Datenschutzgarantien und schliessen einen schriftlichen Auftragsverarbeitungsvertrag ab.

Datenspeicherung in der Schweiz	Wir speichern Personendaten möglichst in der Schweiz. Besonders schützenswerte Personendaten werden ausschliesslich in der Schweiz gespeichert.
Übermittlungen ausserhalb der Schweiz und der EU	Wir übermitteln Personendaten an Drittparteien in ein unsicheres Land ausserhalb der Schweiz und/oder der EU, welches keinen angemessenen Datenschutz gewährleistet, nur, wenn wir geeignete Sicherheitsmassnahmen getroffen haben.

Die Bedeutung und Anforderungen der Datenschutzprinzipien, die stets durch Dimedio und ihre Mitarbeitenden zu beachten sind, werden nachfolgend näher erläutert.

3.1. Rechtmässigkeit der Verarbeitung (Rechtsgrundlage)

a. Personendaten dürfen nur rechtmässig verarbeitet werden. Dies ist der Fall, wenn mindestens eine der folgenden Rechtsgrundlagen gegeben ist:

- Die betroffene Person hat ihre gültige Einwilligung zu der Verarbeitung ihrer Personendaten für den bestimmten Zweck gegeben (z.B. Verarbeitung für Werbezwecke, Newsletters);
- Die Verarbeitung ist für die Erfüllung eines Vertrages mit der betroffenen Person notwendig, oder sie ist zur Durchführung von vorvertraglichen Massnahmen, welche auf Anfrage der betroffenen Person erfolgen, erforderlich (z.B. Erstellung von Angeboten, Versand von gekauften Produkten an die Adresse des Käufers; Datenerhebung und Verarbeitung des Mitarbeitenden für die Erfüllung des Arbeitsvertrages (vgl. weitere Ausführungen in Artikel 3.1. lit. c.);
- Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der Dimedio unterliegt (z.B. Aufbewahrungspflichten aus dem Zivilrecht oder Steuerrecht);
- Die Verarbeitung ist zur Wahrung der berechtigten Interessen von Dimedio erforderlich. Eine Verarbeitung aufgrund berechtigter Interessen kann nur erfolgen, sofern im Einzelfall die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz der Personendaten erfordern, nicht überwiegen. Dabei ist auf die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu Dimedio beruhen, zu berücksichtigen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen und zu dokumentieren. Beispiele berechtigter Interessen können sein: Schutz von Mitarbeitenden und ihren Personendaten, Schutz unserer Geschäftsgeheimnisse und Vermögenswerte, Sicherheit unserer Systeme und Gebäude, Aufrechterhaltung und effiziente Organisation des Geschäftsbetriebs, Verbesserung und Entwicklung unserer Produkte und Leistungen, Einhaltung der rechtlichen und regulatorischen Anforderungen, Verhinderung von Betrug, Vergehen und Verbrechen sowie Untersuchungen im Zusammenhang mit solchen Delikten und sonstigem unangebrachtem Verhalten, Mitwirkung an Rechtsverfahren, die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Besteht die Absicht, Personendaten gestützt auf die berechtigten Interessen zu erheben und zu verarbeiten, ist die Kontaktstelle für Datenschutz zu kontaktieren.

b. Datenverarbeitung im Arbeitsverhältnis/Bewerbung

Im Arbeitsverhältnis dürfen nur die Personendaten erhoben und verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Dabei muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, ausser es liegt ein anderer Grund der Rechtmässigkeit vor (z.B. die Einwilligung des Mitarbeitenden oder ein berechtigtes Interesse von Dimedio).

Im Bewerbungsverfahren dürfen die Personendaten erhoben werden, die für die Beurteilung einer möglichen Eignung des Bewerbenden für eine möglichen Anstellung notwendig sind. Nach Ablehnung sind die Personendaten unter Berücksichtigung beweisrechtlicher Fristen zu löschen. Möchte die Dimedio die Personendaten für eine spätere Position oder ein anderes Bewerbungsverfahren behalten, ist die Einwilligung des Kandidaten/der Kandidatin unter Mitteilung der Aufbewahrungsdauer (z.B. für weitere 12 Monate) notwendig. Die Einholung von Referenzen von ehemaligen Arbeitgebern oder Registerauszüge (z.B. Strafregisterauszug) bedarf grundsätzlich der Zustimmung des Kandidaten/der Kandidatin oder einer gesetzlichen Grundlage.

c. Durchführung Kontrollmassnahmen

Kontrollmassnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen grundsätzlich nur durchgeführt werden, wenn eine gesetzliche Verpflichtung besteht oder ein legitimer Zweck gegeben ist. Ferner müssen die Kontrollmassnahmen geeignet und erforderlich (mildestes Mittel) sein, um den legitimen Zweck zu erreichen und dürfen nur durchgeführt werden, wenn sie angemessen sind. Dabei müssen die berechtigten Interessen der Unternehmung gegen ein mögliches Schutzinteresse der von der Massnahme betroffenen Mitarbeitenden am Ausschluss der Massnahme abgewogen werden. Ferner sind die betroffenen Personen darüber zu informieren, ausser es liegt ein besonderer Grund vor, der die Vornahme der Kontrollmassnahme ohne vorherige Information rechtfertigt (z.B. zur Abwendung einer unmittelbar drohenden Straftat im Rahmen einer strafrechtlichen Untersuchung). Die berechtigten Interessen der Unternehmung sowie die möglichen schutzwürdigen Interessen der Mitarbeitenden müssen vor jeder Massnahme festgelegt und dokumentiert werden. Besteht die Absicht, Kontrollmassnahmen durchzuführen, ist die Anlaufstelle für Datenschutz zu kontaktieren.

d. Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, Intranet und Internet sowie Soziale Netzwerke werden den Mitarbeitenden zur Führung des Geschäftsbetriebes als Arbeitsmittel zur Verfügung gestellt. Sie dürfen im Rahmen der geltenden Rechtsvorschriften und der Unternehmungs-Richtlinien genutzt werden.

Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation sowie die Nutzung von Internet und Intranet findet nicht statt. Zur Sicherheit und Abwehr von Angriffen auf die IT-Infrastruktur und einzelnen Mitarbeitenden können Schutzmassnahmen implementiert werden, die bspw. technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Ferner können zu diesem Zweck die Nutzung der IT-Infrastruktur zeitlich befristet protokolliert werden (sog. Logfiles). Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten und begründeten Verdacht eines Verstosses gegen das Gesetz oder die Richtlinien von Dimedio unter Einhaltung der gesetzlichen Vorschriften wie in Art. 3.1. lit. d durchgeführt werden. Wenn die Absicht besteht, in einem konkreten Fall personenbezogene Auswertungen durchzuführen, ist die Stelle für Datenschutz zu kontaktieren.

Bei Unklarheiten oder Fragen zur Durchführung von Kontrollmassnahmen ist die Anlaufstelle für Datenschutz zu kontaktieren.

3.2. Besonders schützenswerte Personendaten und Persönlichkeitsprofile

Bei der Verarbeitung von besonders schützenswerten Personendaten sind folgende, strengere Anforderungen zu beachten:

a. Sensitive Personendaten: die Verarbeitung von sensitiven Personendaten ist grundsätzlich verboten, es sei denn:

- die betroffene Person hat in der Datenverarbeitung explizit eingewilligt;
- die Verarbeitung ist erforderlich, um rechtliche Pflichten zu erfüllen, insbesondere in den Bereichen des Arbeitsrechts sowie des Rechts der sozialen Sicherheit und des Sozialschutzes; oder
- die Verarbeitung wurde explizit durch die Anlaufstelle für Datenschutz bewilligt.

b. Personendaten von Kindern: Personendaten von Kindern (Kinder unter 16 Jahren) bedürfen zur Rechtmässigkeit der Verarbeitung der Einwilligung bzw. Zustimmung durch den Träger der elterlichen Verantwortung oder einer gesetzlichen Grundlage (z.B. der Vater oder die Mutter), welche die Verarbeitung ausdrücklich erlaubt.

c. Personendaten über Straftaten und/oder Verurteilungen: Personendaten über Straftaten und/oder Verurteilungen dürfen nur verarbeitet werden, wenn dies gesetzlich notwendig oder zulässig ist.

Darüber hinaus unterliegen diese Kategorien von Personendaten besonderen Schutz- und Sicherheitsvorkehrungen, die in der strengsten Form umgesetzt werden müssen, um die Personendaten insbesondere vor unbefugter Verarbeitung, Zugriff sowie Offenbarung zu schützen (z.B. Verschlüsselung, minimale Zugriffsberechtigungen; vgl. dazu Ziff. 3.8.). Bei Unklarheiten oder Fragen zur Erhebung, Verarbeitung oder Sicherstellung dieser Kategorien von Personendaten ist die Anlaufstelle für Datenschutz zu kontaktieren.

Dasselbe gilt für Angaben, welche Rückschlüsse auf wesentliche Eigenschaften von Personen, wie etwa Charaktereigenschaften, erlauben (sogenannte Persönlichkeitsprofile). Dies kann etwa bei Bewerbungsdossiers der Fall sein.

Wenn Sie solche Personendaten beschaffen, müssen Sie die betroffene Person vorgängig darüber informieren (vgl. Artikel 3.3). Wenn Sie dies aus einem bestimmten Grund in einem konkreten Fall nicht als angezeigt erachten, wenden Sie sich bitte an die Anlaufstelle für Datenschutz. Diese wird dann prüfen, ob es gerechtfertigt werden kann, die betroffene Person nicht oder erst später zu informieren.

3.3. Fairness und Transparenz

Die betroffene Person ist bei der Erhebung der Personendaten umfassend, nach Treu und Glauben, sowie in transparenter Weise über die Datenverarbeitung zu informieren. Die Informationen sind in einer verständlichen und leicht zugänglichen Form sowie in einer klaren und möglichst einfachen Sprache zu verfassen. Die Informationen haben mindestens die Angaben in Anhang 1 dieser Richtlinie zu enthalten.

Die Informationen sind in schriftlicher, elektronischer, über die Website, in Applikationen (Apps) (z.B. mittels einer Datenschutzrichtlinie und ggf. Cookie-Hinweisen) oder in anderer geeigneter Form mitzuteilen und zu Beweiszwecken zu dokumentieren.

Auf der Website oder bei Apps ist die Datenschutzrichtlinie (inkl. Cookie-Hinweise) so zu integrieren, dass diese für die Nutzer bzw. die betroffenen Personen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar ist.

Werden zur Auswertung des Nutzerverhaltens von Websiten oder Apps Nutzerprofile erstellt (Tracking), so sind die betroffenen Personen darüber in der Datenschutzrichtlinie zu informieren. Zudem darf ein personenbezogenes Tracking nur erfolgen, wenn dies gesetzlich zulässig ist oder die betroffene Person eingewilligt hat. Werden auf Websiten oder bei Apps in einem registrierungs-/anmeldepflichtigen Bereich Zugriffe auf Personendaten ermöglicht, so sind die Identifizierung (z.B. Nutzername) und Authentifizierung (z.B. Passwort) der betroffenen Personen so zu gestalten, dass ein für den jeweiligen Zugriff angemessener Datenschutz erreicht wird.

Werden die Personendaten nicht direkt bei der betroffenen Person, sondern über einen Dritten erhoben, ergreifen wir angemessene Massnahmen, um sicherzustellen, dass der Dritte die notwendigen Informationen gemäss dieser Richtlinie der betroffenen Person mitgeteilt hat. In jedem Fall stellen wir sicher, dass die Informationen der betroffenen Person spätestens ein Monat nach Erhalt der Personendaten mitgeteilt werden.

Ausnahmsweise müssen die Informationen gemäss Anhang 1 nicht mitgeteilt werden, wenn eine der folgenden Voraussetzungen erfüllt ist:

- die betroffene Person verfügt bereits über die Informationen;
- die Erteilung dieser Informationen erweist sich als unmöglich oder würde einen unverhältnismässigen Aufwand erfordern;
- die Erlangung oder Offenlegung der Personendaten ist ausdrücklich gesetzlich geregelt; oder
- die Personendaten gemäss Gesetz dem Berufsgeheimnis oder einer anderen besonderen Geheimhaltungspflicht unterliegen und daher vertraulich zu behandeln sind.

Bei Unklarheiten oder Fragen zu den Informationspflichten ist die Anlaufstelle für Datenschutz zu kontaktieren.

3.4. Zweckbindung

Personendaten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden, welche:

- der betroffenen Person vorgängig in transparenter Weise mitgeteilt wurden;
- für die betroffene Person aufgrund der Umstände klar erkennbar sind; oder
- gesetzlich vorgeschrieben sind.

Personendaten dürfen nicht für andere, mit diesen nicht zu vereinbarenden Zwecken, weiterverarbeitet werden. Eine Datenerhebung ohne Zweck, wie beispielsweise die Speicherung von Daten auf Vorrat, ist unzulässig.

Besteht die Absicht, die Personendaten für andere, als für die ursprünglich festgelegten Zwecke weiterzuverarbeiten, sind die betroffenen Personen vorgängig über die neuen Zwecke zuzüglich aller anderen massgeblichen Informationen gemäss Anhang 1 zu informieren und soweit notwendig, die Einwilligung einzuholen.

Besteht die Absicht, die Personendaten für andere als für die ursprünglich festgelegten Zwecke zu nutzen und ist unklar, ob die neuen Zwecke mit den ursprünglichen Zwecken vereinbar sind, ist die Anlaufstelle für Datenschutz zu kontaktieren.

3.5. Datenminimierung, Data Protection by Design and by Default

Die Personendaten müssen dem Zweck angemessen sein und auf das für die Zwecke der Verarbeitung notwendige Mass beschränkt sein. Falls möglich, sollte auf eine personenbezogene Verarbeitung verzichtet werden und stattdessen, wo immer möglich und sinnvoll, die Personendaten pseudonymisiert oder anonymisiert werden (z.B. bei statistischen Auswertungen oder Befragungen).

Gleiches gilt für die Auswahl von Datenverarbeitungssystemen. Der Datenschutz ist von Beginn an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Grundsätze des Datenschutzes und des Schutzes der Privatsphäre soweit wie möglich einzuhalten, insbesondere auch den Grundsatz der Datenminimierung.

3.6. Richtigkeit

Die Personendaten müssen sachlich richtig, vollständig und, soweit notwendig, auf dem neusten Stand sein. Es sind alle angemessenen Massnahmen zu treffen, damit die Personendaten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig, unvollständig oder veraltet sind, umgehend gelöscht, berichtigt, ergänzt oder aktualisiert werden.

3.7. Speicherbegrenzung

Personendaten dürfen nur so lange verarbeitet werden, als dies für die Erreichung des Zwecks, für die sie erhoben wurden, notwendig ist, es sei denn, eine längere Aufbewahrung ist aus folgenden Gründen notwendig:

- zur Erfüllung von gesetzlichen Pflichten (z.B. Aufbewahrungs- und Dokumentationspflichten beispielsweise aus dem Zivilrecht oder dem Steuerrecht);
- zur Erfüllung von vertraglichen oder vorvertraglichen Pflichten (z.B. Erstellung eines Arbeitszeugnisses); oder
- zur Erfüllung von berechtigten Geschäftsinteressen von Dimedio (z.B. Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen).

Diesfalls sind geeignete technische und organisatorische Massnahmen durchzuführen (z.B. Pseudonymisierung, Beschränkung auf einen sehr kleinen Personenkreis), um die Personendaten angemessen zu schützen.

3.8. Vertraulichkeit und Integrität

Die Personendaten müssen im Umgang vertraulich behandelt werden und in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Personendaten gewährleistet, einschliesslich Schutz vor unbefugter oder unrechtmässiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter/eine Mitarbeiterin vornimmt, ohne damit im Rahmen der Aufgabenerfüllung betraut und entsprechend berechtigt zu sein (z.B. unbefugte Übermittlung der Personendaten oder das Zugänglichmachen an unbefugte Mitarbeitende oder Dritte oder die Nutzung für eigene private Zwecke). Mitarbeitende dürfen nach dem Need-to-Know Prinzip nur Zugang zu Personendaten haben, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Zu diesem Zweck treffen wir

geeignete technische und organisatorische Massnahmen, welche insbesondere folgende Massnahmen eischliesst:

- Pseudonymisierung und Verschlüsselung der Personendaten: Wir werden die Personendaten pseudonymisieren, verschlüsseln oder auf anderer Weise identifizierbare Informationen durch ein Code ersetzen, um eine Identifikation des Betroffenen zu verhindern, soweit dies vernünftigerweise möglich und angemessen ist;
- Sicherstellung der andauernden Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der Personendaten;
- Sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten nach dem Need-to-Know-Prinzip;
- Rasche Wiederherstellung der Verfügbarkeit der Personendaten und des Zugangs zu ihnen bei einem physischen oder technischen Zwischenfall;
- Privacy by Design and by Default: Wir werden bereits bei der Festlegung der Mittel für die Datenverarbeitung wie auch beim Design neuer Produkte, Dienstleistungen und Nutzung von neuen Technologien den Datenschutz und den Schutz der Rechte und Freiheiten der betroffenen Personen genügend berücksichtigen. Wir werden nur Personendaten erheben und nutzen, welche für den bestimmten Verarbeitungszweck tatsächlich erforderlich sind. Ferner werden wir den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit auf das Nötigste beschränken;
- Implementierung eines Prozesses zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen, um die Sicherheit der Datenverarbeitung zu gewährleisten.

3.9. Nutzung von Auftragsverarbeitern

Eine Auftragsverarbeitung liegt vor, wenn ein Dritter (Auftragsverarbeiter) in unserem Auftrag und auf unsere Anweisung hin Personendaten für uns verarbeitet, ohne dass dem Auftragsverarbeiter die Verantwortung über den betroffenen Geschäftsprozess übertragen wird, d.h. die gesamte Verantwortung über die korrekte Durchführung der Datenverarbeitung bleibt bei uns als Auftragsgeber. Der Auftragsverarbeiter darf die Personendaten nur im Rahmen unserer Weisungen verarbeiten. Befindet sich der Auftragsverarbeiter ausserhalb der Schweiz oder der EU, sind die Anforderungen gemäss nachfolgendem Artikel 3.10. zu beachten. Bei einer Auftragsverarbeitung müssen folgende Bedingungen erfüllt sein:

- Der Auftragsverarbeiter muss sorgfältig auf hinreichende Schutzgarantien geprüft werden, wonach dieser geeignete technische und organisatorische Massnahmen so durchführt, dass die Verarbeitung der Personendaten im Einklang mit dieser Richtlinie und den Anforderungen des anwendbaren Datenschutzgesetzes erfolgt und der Schutz der Rechte der betroffenen Personen gewahrt ist. Die Prüfung der Schutzgarantien sollte auch während einer Zusammenarbeit regelmässig wiederholt werden;
- Mit jedem Auftragsverarbeiter muss ein schriftlicher Auftragsverarbeitungsvertrag abgeschlossen werden, in dem u.a. Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der Personendaten, die Kategorien betroffener Personen, die Gewährleistung der Datensicherheit durch Umsetzung geeigneter technischen und organisatorischen Massnahmen sowie weitere Pflichten des Auftragsverarbeiters regelt.

Wenn die Absicht besteht, Personendaten an einen Auftragsverarbeiter auszulagern (Outsourcing), ist die Anlaufstelle für Datenschutz zu kontaktieren.

3.10. Übermittlungen ausserhalb der Schweiz und der EU

Werden Personendaten an Dritte übermittelt (z.B. Tochtergesellschaft, Vertragspartner, Behörde), darf dies nur rechtmässig, bei Vorliegen eines Rechtsgrundes gemäss Ziffer 3.1., erfolgen (z.B. Vertrag, Gesetz, oder Einwilligung). Zudem muss der Empfänger verpflichtet werden, die Personendaten nur zu den festgelegten Zwecken zu verwenden.

Übermittlungen von Personendaten ausserhalb der Schweizer und der EU in ein Drittland mit einem unangemessenen Datenschutzniveau, dürfen nicht erfolgen, es sei denn, der betroffenen Person stehen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung und Dimedio hat angemessene Schutzgarantien vorgesehen, wie bspw.:

- EU-Standarddatenschutzklauseln;
- Verbindliche interne Datenschutzvorschriften;
- Genehmigte Verhaltensregeln (Code of Conduct);
- Genehmigtes Zertifizierungsmechanismus; oder
- Bei Vorliegen einer Ausnahme für bestimmte Fälle (z.B. ausdrückliche Zustimmung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen).

Wenn die Absicht besteht, Personendaten ausserhalb der Schweiz und der EU zu transferieren oder an einen Dritten, der ausserhalb der Schweiz und der EU ansässig ist, Zugriff auf die Personendaten zu geben, ist die Anlaufstelle für Datenschutz zu kontaktieren.

4. Rechte der betroffenen Personen

Wir verarbeiten die Personendaten stets im Einklang mit den Rechten der betroffenen Person. Die betroffene Person hat insbesondere folgende Rechte:

4.1. Recht auf Information

Die betroffene Person hat das Recht, in transparenter Weise über die Personendaten, die von ihr verarbeitet werden, informiert zu werden. Die Informationen, welche der betroffenen Person bei der Datenerhebung mitgeteilt werden müssen, sind im Anhang I dieser Richtlinie aufgeführt.

4.2. Recht auf Auskunft

Die betroffene Person hat das Recht, von uns eine Bestätigung darüber zu verlangen, ob sie betreffende Personendaten verarbeitet werden. Bei einem entsprechenden Antrag sind gegenüber der beantragenden Person grundsätzlich die in Anhang II aufgeführten Informationen mitzuteilen.

Die zuständige Person bei Dimedio stellt eine Kopie der Personendaten, die Gegenstand der Verarbeitung sind, kostenlos zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann eine angemessene Entschädigung auf der Grundlage der Verwaltungskosten verlangt werden.

Stellt die betroffene Person einen Antrag in elektronischer Form, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt. In jedem Fall zu beachten ist, dass durch die Auskunftserteilung keine Rechte und Freiheiten anderer Personen beeinträchtigt werden.

4.3. Recht auf Berichtigung, Vervollständigung und Löschung

Die betroffene Person hat das Recht, vom Verantwortlichen unverzüglich die Berichtigung sie betreffender Personendaten zu verlangen, wenn sich diese als unrichtig erweisen. Ebenso können sie die Vervollständigung unvollständiger Personendaten verlangen. Darüber hinaus können sie bei gegebenen Voraussetzungen die Löschung ihrer Daten beantragen.

4.4. Recht auf Widerspruch und Einschränkung

Die betroffene Person hat das Recht, der Verarbeitung ihrer Personendaten aus berechtigten Gründen zu widersprechen und vom Verantwortlichen bei gegebener Voraussetzung die Einschränkung der Verarbeitung zu verlangen.

4.5. Recht auf Datenübertragbarkeit

Die betroffene Person hat bei gegebenen Voraussetzungen das Recht, die sie betreffenden Personendaten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und diese einem anderen Verantwortlichen, zu übermitteln.

4.6. Widerspruchsrecht bei Direktwerbung (einschliesslich Profiling)

Wenn Personendaten verarbeitet werden, um Direktwerbung (einschliesslich Profiling) zu betreiben, so hat die betroffene Person das Recht, jederzeit dieser Datenverarbeitung zu widersprechen.

4.7. Recht, nicht Gegenstand einer automatisierten Entscheidung im Einzelfall (einschliesslich Profiling) zu sein

Die betroffene Person hat das Recht, nicht einer ausschliesslich auf einer automatisierten Verarbeitung (einschliesslich Profiling) beruhenden Entscheidung (d.h. die Entscheidung erfolgt auf Grundlage einer automatisierten maschinellen Verarbeitung ohne Mitwirkung einer natürlichen Person, z.B. automatische Ablehnung im Online-Bewerbungsverfahren) unterworfen zu werden, wenn diese ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Eine Ausnahme, bei der ein solches Vorgehen zulässig ist, besteht lediglich in folgenden Fällen:

- eine solche Entscheidung ist notwendig für einen Vertragsabschluss;
- dies ist gemäss anwendbarem Recht zulässig; oder
- die betroffene Person hat dem ausdrücklich zugestimmt.

In diesem Fall treffen wir angemessene Massnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren und räumen ihr mindestens die Möglichkeit ein, gegenüber einer natürlichen Person die Entscheidung anzufechten und ihren Standpunkt darzulegen.

4.8. Umgang und Antworten auf solche Anfragen

Dimedio stellt sicher, dass die genutzten Systeme und Prozesse im Einklang mit den Anforderungen zur Gewährleistung der Rechte der betroffenen Personen stehen.

Bei der Bearbeitung von Anträgen ist die Identität der betroffenen Person zweifelsfrei festzustellen. Bei begründeten Zweifeln an der Identität können zusätzliche Angaben vom Antragsteller angefordert werden. Ferner ist zu prüfen, ob aufgrund besonderer Umstände und gegebener Voraussetzungen, die Beantwortung eines entsprechenden Antrags gegebenenfalls verzögert, beschränkt oder verweigert werden muss.

Die betroffene Person ist spätestens innerhalb eines Monats über alle ergriffenen Massnahmen, die auf ihren Antrag hin erfolgt sind, zu informieren.

Entsprechende Anträge von betroffenen Personen sind umgehend an die Anlaufstelle für Datenschutz weiterzuleiten.

5. Sicherheitsvorkehrungen im IT-Bereich

Dimedio ergreift sämtliche technisch möglichen und verhältnismässigen Massnahmen, um die ihr anvertrauten, personenbezogenen Daten zu schützen.

Insbesondere gelten bei Dimedio folgende Vorgaben:

- Alle Systemzugänge sind mit einem persönlichen, sicheren Passwort zu schützen.
  Die Passwörter müssen sicher aufbewahrt werden und dürfen nicht allgemein zugänglich sein.
- Die Verwendung von allgemeinen Passwörtern ist untersagt.
- Wenn systemtechnisch möglich, ist die Zwei-Faktoren-Authentifizierung zu aktivieren.

6. Zuständigkeit Datenschutz

Für den Datenschutz bei Dimedio ist die Geschäftsleitung zuständig. Sie ist die interne Anlaufstelle für den Datenschutz.

7. Meldung einer Datenschutzverletzung

Alle Mitarbeitenden unverzüglich eine mögliche Verletzung dieser Datenschutzrichtlinie oder der Sicherheit der Personendaten, welche zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zum unbefugten Zugang zu Personendaten führt, der Anlaufstelle für Datenschutz melden.

Die Anlaufstelle für Datenschutz wird den Vorfall auf Verletzung des Datenschutzes hin prüfen und soweit erforderlich, die mögliche Verletzung den zuständigen Aufsichtsbehörden und den betroffenen Personen melden und alle weiteren Schritte gemäss Datenschutzgesetzgebung vornehmen, um die Auswirkungen der Datenschutzverletzung für die betroffenen Personen und die Unternehmung soweit wie möglich zu minimieren.

8. Kontrolle und Sanktionen

Die Einhaltung dieser Richtlinie und der geltenden Datenschutzgesetze wird regelmässig durch die Geschäftsleitung überprüft.

Die Einhaltung dieser Richtlinie ist von grosser Wichtigkeit für Dimedio. Die Nichteinhaltung kann zu erheblichen Haftungs- und Schadensansprüchen gegen Dimedio führen. Aus diesem Grunde kann die Nichtbeachtung oder ein Verstoss gegen diese Richtlinie arbeitsrechtliche Massnahmen (einschliesslich einer fristlosen oder ordentlichen Kündigung), wie auch straf- und/oder zivilrechtliche Sanktionen und Schadenersatz zur Folge haben.

9. Implementierung und Änderungen

Diese Richtlinie tritt am 1. September 2023 in Kraft. Sie wird regemässig überprüft und kann jederzeit mit sofortiger Wirkung angepasst werden. Die Mitarbeitenden werden bei einer Anpassung per Email oder auf andere geeignete Weise informiert.

Anhang I – Recht auf Information

Wenn wir Personendaten erheben, teilen wir der/n betroffenen Person/en vor dem Zeitpunkt der Erhebung im Minimum Folgendes mit:

Mindestinformationen gemäss Art. 19 Abs. 2 nDSG:

a. Die Identität und die Kontaktdaten der Dimedio GmbH;

b. Den Bearbeitungszweck;

c. Die Kategorien der betroffenen Personendaten, die von den betroffenen Personen erhoben werden, falls die Personendaten nicht direkt von der betroffenen Person beschafft werden (z.B. von einer Drittunternehmung) und somit für diese nicht erkennbar ist;

f. Gegebenenfalls die Empfänger oder Kategorien von Empfänger, denen Personendaten bekanntgegeben werden; und

g. Werden die Personendaten ins *Ausland* bekanntgegeben, so teilt er der betroffenen Person auch den *Staat oder das internationale Organ* und gegebenenfalls die Garantien nach Artikel 16 Absatz 2 oder die Anwendung einer Ausnahme nach Artikel 17 mit.

Anhang II – Recht auf Auskunft

1. Mindestinformationen gemäss Art. 25 Abs. 2 nDSG:

Bei einer Antragstellung auf Auskunft durch die betroffene Person über die von ihr verarbeitete Personendaten, sind der betroffenen Person gemäss Art. 25 Abs. 2 nDSG mindestens folgende Informationen mitzuteilen, sofern keine Einschränkung des Auskunftsrechts gemäss Art. 26 nDSG vorliegt:

a. die Identität und die Kontaktdaten des Verantwortlichen;

b. Die bearbeiteten Personendaten als solche;

c. Der Bearbeitungszweck

d. Die Aufbewahrungsdauer der Personendaten, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

c. die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person beschafft wurden;

d. gegebenenfalls das Vorliegen einer automatisierten Einzelentscheidung sowie die Logik, auf der die Entscheidung beruht;

e. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden, sowie die Informationen zu einer Auftragsbearbeitung, falls die Personendaten an einen Auftragsbearbeiter ausgelagert werden.

2. Weitere Informationen zur Gewährleistung einer transparenten und fairen Datenbearbeitung

Darüber hinaus sind gemäss Art. 25 Ziff. 2 weitere Informationen der betroffenen Person mitzuteilen, damit sie ihre Rechte nach dem Datenschutzgesetz geltend machen kann und eine transparente Datenbearbeitung gewährleiste ist, wie bspw. folgende Informationen:

a. Das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden Personendaten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

b. Das Recht, bei der zuständigen Aufsichtsbehörde eine Beschwerde einzureichen;

c. Sofern Personendaten ins Ausland transferiert werden, so hat die betroffene Person das Recht, über die angemessenen Garantien informiert zu werden, die einen angemessenen Datenschutz gewährleisten sollen.