Erarbeitet durch DATA Security AG

Leitlinie zum Datenschutz

Stand: 05.11.2023

Inhaltsverzeichnis

I. Präambel

Das Bundesamt für Justiz hat am 3. März 2022 bekannt gegeben, dass das revidierte Datenschutzgesetz 1. September 2023 in Kraft tritt. Das Bundesgesetz über den Datenschutz strebt den Schutz der Persönlichkeit und der Grundrechte von Personen an, über die Daten bearbeitet werden. Es regelt die Handhabung von Daten, die von Privatpersonen und Bundesorganen bearbeitet werden. Der eidgenössische Datenschutzberater hat die Einhaltung des Gesetzes zu überwachen. In 17 Kantonen bestehen auch kantonale Regelungen über den Datenschutz.

Diese Leitlinie versteht sich als eine Selbstverpflichtung unserer Organisation zur Einhaltung des Datenschutzes. Die Themen "gesetzlicher Datenschutz und Informationssicherheit" werden für uns und unsere Mandanten immer wichtiger und bedeutsamer.

Als Organisation geniessen wir ein hohes Vertrauen unserer Mandanten. Vertrauen bedeutet jedoch auch Verantwortung für unser Handeln, für unsere Arbeit, für die Systeme und Daten der Mandanten.

Unsere Mandanten legen Ihre persönlichen und betriebswirtschaftlichen Daten in unsere Hände, und damit auch alle organisationswichtigen sowie kritischen Informationen.

Für uns in der STARTNOW.SUPPORT AG ist es besonders wichtig, mit diesen Daten verantwortungsbewusst umzugehen. Daher liegt es nahe, dass wir das Thema "gesetzlicher Datenschutz" in der Praxis sehr ernst nehmen und uns auch entsprechend organisieren.

Diese Leitlinie soll helfen, die Bedeutung und Wichtigkeit des gesetzlichen Datenschutzes hervorzuheben, um die Transparenz dieses Themas für unsere Mitarbeitern zu erhöhen.

II. Zweck und Selbstbild

Die Gesetze und Bestimmungen zum Datenschutz und zur Datensicherheit haben zum Ziel, das Verarbeiten von personenbezogenen Daten nur dann zu erlauben, wenn hierfür ein begründeter und legitimer Zweck gegeben ist.

Wenn Personendaten innerhalb unserer Organisation gesammelt, verarbeitet (d.h. auch übermittelt) oder benutzt werden, muss hierbei von allen Beteiligten ein adäquates Datenschutzniveau gewährleistet werden.

Diese Leitlinie bildet die Grundlage für die Erstellung weiterer, auch fachspezifischer Richtlinien, Datenschutzkonzepte und detaillierter Regelungen sowie Arbeitsanweisungen zum Datenschutz und zur Datensicherheit.

Um den gesetzlichen Anforderungen zu entsprechen, bilden die Leitlinie sowie alle zusammenhängenden und erforderlichen Dokumente und Prozesse den Rahmen unseres Datenschutzmanagements.

III. Zielvorgaben

Das Thema Datenschutz ist in der STARTNOW.SUPPORT AG allgegenwärtig. Datenschutz bedeutet Schutz der Personen, die sich hinter der Organisation gespeicherten und zu verarbeiteten Daten verbergen. Unsere Datenschutzleitlinie soll die Grundrechte und Grundfreiheiten von Betroffenen, insbesondere ihr Recht auf Schutz personenbezogener Daten, wahren und schützen.

Die Wahrung des Datenschutzes ist ausserdem eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation der STARTNOW.SUPPORT AG als attraktiver Arbeitgeber.

Beim Umgang mit personenbezogenen Daten müssen neben anderen Gesetzen und Vorschriften hauptsächlich die Bestimmungen der revDSG beachtet werden. Verantwortliches Handeln beim Umgang mit personenbezogenen Daten, aber auch die risikobewusste Nutzung von IT-Systemen und -Anwendungen sind die zentralen Zielsetzungen.

Durch die sogenannte Datenschutz-Compliance wollen wir gegenüber allen Betroffenen ein Qualitätsmerkmal ausdrücken. Die Organisation möchte den Verpflichtungen aus den rechtlichen Vorgaben zum Datenschutz (revDSG) nachkommen, und sorgt für ihre Durchsetzung.

Dazu hat sich die Organisation folgende Ziele gesetzt:

- Einhaltung datenschutzrechtlicher Anforderungen, insbesondere die Erfüllung der Anforderungen nach den revDSG Normen;
- Sicherstellung einer vertrauensvollen und datenschutzgerechten Verarbeitung von Daten;
- Minimierung der Risiken und Schäden, denen betroffene Personen ausgesetzt sein könnten;
- hohe Verlässlichkeit der Datenverarbeitung, insbesondere hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sowie bei der raschen Wiederherstellung der Verfügbarkeit;
- Sicherstellung geeigneter technischer und organisatorischer Massnahmen, inklusive Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser Massnahmen;
- Wahrung der Reputation in der Öffentlichkeit.

Diese Ziele leiten sich ebenfalls aus den Geschäftszielen und der Organisationsstrategie ab und stimmen mit diesen überein.

Die Geschäftsführung ist für die Überprüfung der Ziele und Zielvorgaben zuständig. Sie bewertet die Erreichung der Zielvorgaben.

IV. Chancen

Durch die Etablierung eines Datenschutz-Managementsystems (DSMS) werden Personendaten, Prozesse und Systeme identifiziert, begutachtet und Verantwortlichkeiten erkannt.

Dadurch wird auch die Erfüllung der Anforderungen unserer Rechenschaftspflichten gewährleistet. Die Rechenschafts- und Nachweispflichten werden durch eine ausführliche Dokumentation erfüllt.

Die ständige Überprüfung und kontinuierliche Verbesserung innerhalb des DSMS ermöglicht es, neuen Risiken zu begegnen, neue Anforderungen zu identifizieren und zu erfüllen, und damit die Qualität des Systems zu erhöhen.

Zudem werden dadurch nicht nur die gesetzlichen Vorgaben erfüllt, sondern unsere Organisation erhält die Chance, eigene Prozesse besser zu steuern und zu optimieren.

V. Geltungsbereich

Diese Leitlinie erstreckt sich auf das DSMS und gilt für die gesamte Organisation.

Die Geschäftsführung erwartet, dass alle Mitarbeiter, externe Parteien und auch die Geschäftsführung selbst diese Leitlinie und alle dazugehörigen Regeln, Verhaltensanforderungen und Dokumente bzw. Dokumentationspflichten beachten und einhalten.

VI. Datenschutzprinzipien

Durch die revDSG ergeben sich bei der Verarbeitung von personenbezogenen Daten eine Reihe von Pflichten.

Die Rede ist u.a. von Auskunfts-, Berichtigungs-, Sperrungs- und Löschungspflichten gegenüber den Betroffenen sowie Verpflichtungen auf den sorgsamen Umgang mit personenbezogenen Daten bei allen Personen, die mit personenbezogenen Daten umgehen.

Die hierbei führenden Prinzipien, auf die näher einzugehen ist, ergeben sich aus Art. 6 revDSG:

1. Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personendaten müssen auf rechtmässige Weise erhoben und verarbeitet werden.

Ein Betroffener muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind Personendaten beim Betroffenen selbst zu erheben.

2. Zweckbindung

Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

3. Datenminimierung

Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang die Datenerhebungen notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen.

Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden.

Personendaten dürfen nicht auf Vorrat für zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

4. Richtigkeit

Personendaten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Massnahmen zu treffen, um sicherzustellen, dass nicht zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

5. Speicherbegrenzung

Personendaten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt wurde, oder unsere Organisationsarchive den Datenbestand auf seine Archivwürdigkeit für historische Zwecke bewerten konnten.

6. Integrität und Vertraulichkeit

Für Personendaten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Massnahmen gegen unberechtigten Zugriff, unrechtmässige Verarbeitung oder Weitergabe sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

7. Rechenschaftspflichtigkeit

STARTNOW. SUPPORT AG ist für die Einhaltung der Grundsätze rechenschaftspflichtig. Die Einhaltung muss nachgewiesen werden können. Beim Datenschutz erfolgt eine "Beweislastumkehr", d.h. unsere Organisation muss aktiv und unabhängig davon, ob es überhaupt zu Schäden oder Verstössen kam, nachweisen, dass der Datenschutz funktioniert. Dabei genügt es dann nicht mehr, die Prozesse lediglich im Griff zu haben. Stattdessen ist deren Funktionsfähigkeit aktiv nachzuweisen.

Die Einhaltung der Vorschriften der revDSG, haben in unserer Organisation einen hohen Stellenwert.

VII. Begriffsbestimmung

Durch die revDSG ergeben sich bei der Verarbeitung von personenbezogenen Daten eine Reihe von Pflichten.

Die Rede ist u.a. von Auskunfts-, Berichtigungs-, Sperrungs- und Löschungspflichten gegenüber den Betroffenen sowie Verpflichtungen auf den sorgsamen Umgang mit personenbezogenen Daten bei allen Personen, die mit personenbezogenen Daten umgehen.

Die hierbei führenden Prinzipien, auf die näher einzugehen ist, ergeben sich aus Artikel 5 revDSG:

1. Personendaten

Personendaten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Betroffener). Mandantendaten gehören dabei ebenso zu den Personendaten wie Personaldaten von Beschäftigten. Beispielsweise lässt der Name eines Ansprechpartners ebenso einen Rückschluss auf eine natürliche Person zu, wie seine E-Mail-Adresse. Es genügt, wenn die jeweilige Information mit dem Namen des Betroffenen verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann.

Ebenso kann eine Person bestimmbar sein, wenn die Information mit einem Zusatzwissen erst verknüpft werden muss, so zum Beispiel beim Autokennzeichen. Das Zustandekommen der Information ist für einen Personenbezug unerheblich. Auch Fotos, Video- oder Tonaufnahmen können Personendaten darstellen.

2. Besondere Personendaten

Besondere Arten von Personendaten sind Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie eine eventuelle Gewerkschaftszugehörigkeit hervorgehen kann sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung einer natürlichen Person.

3. Bearbeiten/ Verarbeitung

Bearbeiten/Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Personendaten, 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, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

4. Einschränkung der Verarbeitung

Einschränkung der Verarbeitung ist die Markierung gespeicherter Personendaten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

5. Pseudonymisierung

Pseudonymisierung ist die Verarbeitung Personendaten in einer Weise, dass die Personendaten 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 Personendaten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

6. Auftragsbearbeiter

Auftragsbearbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die Personendaten im Auftrag des Verantwortlichen verarbeitet.

7. Empfänger

Empfänger ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der Personendaten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

8. Dritter

Dritter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, ausser der betroffenen Person, dem Verantwortlichen, dem Auftragsbearbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsbearbeiter befugt sind, die Personendaten zu verarbeiten.

9. Einwilligung des Betroffenen

Eine Einwilligung des Betroffenen 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 der Betroffene zu verstehen gibt, dass er mit der Verarbeitung der ihn betreffenden Personendaten einverstanden ist.

VIII. Grundsätzliches

Durch diese Leitlinie wird die datenschutzkonforme Informationsverarbeitung geregelt und die sich daraus ergebenden Verantwortlichkeiten für die STARTNOW. SUPPORT AG klargestellt. Alle Mitarbeiter sind zur Einhaltung der Leitlinie verpflichtet.

Adressaten dieser Leitlinie sind:

- Alle Abteilungen und jeder einzelne Mitarbeiter, die mit der Verarbeitung Personendaten betraut sind.
- Der Datenschutzberater (DSB), der ihre Umsetzung beratend und kontrollierend begleitet und die ihm speziell zugewiesenen Aufgaben wahrzunehmen hat.

Folgende Grundsätze gelten in diesem Zusammenhang:

- Die Hard- und Software zur Datenverarbeitung ist für betriebliche Aufgaben, und zwar für die jeweils vorgesehenen Zwecke, zu verwenden und gegen Verlust und Manipulation zu sichern.
- Alle Mitarbeiter ist in ihrem Verantwortungsbereich für die Umsetzung der Leitlinie verantwortlich. Die Einhaltung muss von ihnen regelmässig kontrolliert werden.
- Die für die jeweilige Datenverarbeitung und die hierfür eingesetzten Systeme Verantwortlichen stellen sicher, dass ihre Mitarbeiter über diese Leitlinie informiert werden.
- Der Datenschutzberater berät bei der Umsetzung der Leitlinie und prüft deren Einhaltung.

Alle Adressaten der Leitlinie sind insoweit dem Datenschutzberater gegenüber auskunftspflichtig.

IX. Datenschutzberater

Die STARTNOW. SUPPORT AG hat nach Massgabe des Artikel 10 revDSG einen betrieblichen Datenschutzberater bestellt. Der Datenschutzberater ist zu erreichen unter dominik.adam@startnow.support.

Seine Kontaktdaten sind auch zu finden unter www.startnow.support. Der Datenschutzberater nimmt die ihm kraft Gesetzes und aus dieser Leitlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seines Fachwissens sowie seiner beruflichen Qualifikation wahr. Er berichtet unmittelbar der Organisationsleitung und ist zuständig für die Kommunikation mit Aufsichtsbehörden.

Der Datenschutzberater unterrichtet und berät die Organisationsleitung sowie die Beschäftigten hinsichtlich ihrer Datenschutzpflichten. Dem Datenschutzberater obliegt die Überwachung der Einhaltung der revDSG und anderer gesetzlicher Vorgaben zum Datenschutz, einschliesslich der Vorgaben dieser Richtlinie, sowie die Überwachung der Strategien von STARTNOW. SUPPORT AG für den Schutz der Personendaten einschliesslich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an Verarbeitungsvorgängen beteiligten Mitarbeiter. Ausgewählte Prozesse werden stichprobenartig, risikoorientiert und in angemessenen Zeitabständen auf ihre Datenschutzkonformität hin kontrolliert. Darüber hinaus steht der Datenschutzberater dem Verantwortlichen bei einer möglichen risikoreichen Datenverarbeitung und der Abschätzung des Risikos beratend zur Seite.

Der Datenschutzberater wird frühzeitig in alle Datenschutzfragen eingebunden. Er wird dabei von der Organisationsleitung und den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt.

Die Organisationsleitung überträgt die Aufgabe des Führens eines Verzeichnisses von Verarbeitungstätigkeiten und des Erteilens von Auskünften auf den Datenschutzberater. Für Meldungen, Auskünfte etc. gegenüber den Datenschutzaufsichtsbehörden bezüglich des Verzeichnisses für Verarbeitungstätigkeiten liegt die Zuständigkeit bei dem Datenschutzberaters.

Der Datenschutzberater berichtet jährlich innerhalb des Managementreviews der Geschäftsführung über seine Tätigkeiten, darunter über stattgefundene Prüfungen, Beanstandungen und ggf. noch zu beseitigende Organisationsmängel.

X. Beschaffung von Hard- und Software

Die Beschaffung von Hard- und Software erfolgt grundsätzlich auf Anforderung der über die Verarbeitungen entscheidenden IT-Betreuer.

Bereits bei der Auswahl von Hard- und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet.

Wenn durch die Beschaffung von Hard- und Software ein neues Verfahren der Verarbeitung von Personendaten eingeführt werden soll, ist Patrick Ernst oder Dominik Adam rechtzeitig vorab von der anfordernden Stelle zu informieren. Die Beschaffung erfolgt erst nach Stellungnahme des Datenschutzberaters. Patrick Ernst oder Dominik Adam berät dahingehend, ob die Durchführung einer Datenschutz-Folgenabschätzung erforderlich ist.

Der Einsatz privater Hard- und Software darf nicht zur Verarbeitung Personendaten verwendet werden. Die dienstliche Nutzung privater Hard- und Software im heimischen und ausserbetrieblichen Bereich (z.B. private Notebooks) bedarf der Genehmigung durch den IT-Betreuer *und die Geschäftsleitung* im Einzelfall.

Die IT-Abteilung führt ein Verzeichnis der eingesetzten Hardware und der verwendeten Anwendungsprogramme. Der Datenschutzberater kann auf das Verzeichnis jederzeit zugreifen.

Bei Verdacht des unbefugten Zugriffs auf Personendaten, der Sabotage, des Diebstahls von Hard- und Software etc. sind die IT-Abteilung, der Datenschutzberater und Geschäftsführer unverzüglich zu informieren.

Wenn es eine Arbeitsanweisung geben sollte, z.B. "Umgang mit Datenpannen", wäre diese hier zu referenzieren.

XI. Verpflichtungen und Mitarbeiter-Schulung

Personendaten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut zu sein und für die keine Rechtsgrundlage besteht. Mitarbeiter dürfen Personendaten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.

Jeder Mitarbeiter, der Zugang zu Personendaten hat, ist auf einen vertraulichen Umgang mit Personendaten zu verpflichten. Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars und unter Aushändigung der Datenschutzleitlinie durch die Organisation.

Der Datenschutzberater ist über die Verpflichtung von Mitarbeitern und deren Arbeitsplatz zwecks von ihm vorzunehmenden weiteren Schulungen und die Feststellung evtl. Kontrollbedarfs zu informieren.

Für in Abstimmung mit den jeweiligen Abteilungsleitungen angesetzte Schulungstermine sind die betroffenen Mitarbeiter freizustellen.

XII. Verzeichnis von Bearbeitungstätigkeiten

Über Verfahren, die den Umgang mit Personendaten betreffen, führt Patrick Ernst oder Dominik Adam ein Verzeichnis von Verarbeitungstätigkeiten gemäss Artikel 12 revDSG.

Der für ein Verfahren Verantwortliche bzw. die zuständige Fachabteilung meldet dieses zeitnah gemäss den vom Patrick Ernst oder Dominik Adam definierten Vorgaben. Gleiches gilt für Veränderungen.

Unabhängig von dieser Meldung ist Patrick Ernst oder Dominik Adam bei der Planung der Einführung neuer Verarbeitungen bzw. der Veränderung bestehender Verfahren über Zweck und Inhalt der Anwendung und die Erfüllung der Benachrichtigungspflicht zu informieren. Bei standardisierten Erhebungen (Fragebögen, Preisausschreiben, Eingabefelder auf der Internet-Homepage etc.) ist der Erhebungsbogen etc. Patrick Ernst oder Dominik Adam zur Abstimmung vorzulegen.

Soweit Patrick Ernst oder Dominik Adam feststellt, dass die beabsichtigte Verarbeitung einer Datenschutz-Folgenabschätzung unterliegt, teilten sie dies umgehend mit. Die Verarbeitung darf erst nach Zustimmung von Patrick Ernst oder Dominik Adam durchgeführt werden. Im Zweifel entscheidet die Geschäftsleitung Patrick Ernst.

XIII. Betroffenenrechte

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen.

Betroffene haben nach den Artikel 25 revDSG das Recht auf Auskunft über die in der Organisation über ihre Person gespeicherten Personendaten.

Bei der Bearbeitung von Anträgen ist die Identität des Betroffenen zweifelsfrei festzustellen. Bei begründeten Zweifeln an der Identität können zusätzliche Angaben vom Antragsteller angefordert werden.

Die Auskunftserteilung erfolgt schriftlich, es sei denn der Betroffene hat den Antrag auf Auskunft elektronisch gestellt. Der Auskunft ist eine Kopie der Daten des Betroffenen beizufügen, die neben den zur Person vorhandenen Daten, auch die Empfänger von Daten, den Zweck der Speicherung sowie alle weiteren gesetzlich geforderten Informationen nach Artikel 25 revDSG beinhaltet, um den Betroffenen die Verarbeitung bewusst zu machen und die Rechtmässigkeit selbst beurteilen zu lassen. Auf besonderen Wunsch des Betroffenen werden die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt. Der IT-Betreuer legt den hierfür vorzusehenden Standard fest.

Betroffene haben nach Artikel 32 revDSG einen Anspruch auf Berichtigung ihrer Personendaten, wenn sich diese als unrichtig erweisen. Ebenso können sie die Vervollständigung unvollständiger Personendaten verlangen.

Der Betroffene hat nach Artikel 32 revDSG/Artikel 17 DS-GVO das Recht auf Löschung seiner Personendaten unter den folgenden Voraussetzungen:

- Die Kenntnis der Daten ist für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich.
- Der Betroffene hat eine Einwilligung widerrufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
- Ihre Verarbeitung ist unzulässig.
- Der Betroffene legt Widerspruch gegen die Verarbeitung zu Zwecken der Werbung und Marktforschung ein oder beruft sich auf ein Widerspruchsrecht aufgrund einer besonderen – zu begründenden – persönlichen Situation.
- Es handelt sich um besondere Personendaten, deren Richtigkeit nicht bewiesen werden kann.
- Es besteht eine anderweitige rechtliche Verpflichtung zur Datenlöschung.

Besteht eine Verpflichtung zur Löschung und wurden die Personendaten zuvor öffentlich gemacht, sind weitere Verantwortliche für die Datenverarbeitung über ein Löschbegehren des Betroffenen hinsichtlich aller Kopien seiner Daten sowie aller Links zu diesen Daten zu informieren.

Der Betroffene kann die Einschränkung der Verarbeitung seiner Daten verlangen, wenn

- die Richtigkeit der Personendaten strittig ist, jedoch nur so lange, wie die Richtigkeit durch die zuständige Fachabteilung überprüft wird; oder
- die Verarbeitung unzulässig ist, der Betroffene die Datenlöschung aber ablehnt; oder
- das Unternehmen die Personendaten für Zwecke der Verarbeitung nicht mehr benötigt, der Betroffene die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt; oder
- der Betroffene Widerspruch gegen die Verarbeitung aufgrund einer besonderen Situation eingelegt hat und die zuständige Fachabteilung noch mit der Prüfung des Widerspruchs befasst ist.

Macht ein Betroffener von seinem Auskunftsrecht nach Artikel 25 revDSG oder seinem Korrektur- oder Widerspruchsrecht nach Artikel 32 rev DSG Gebrauch, so erfolgt die zentrale Bearbeitung durch Patrick Ernst oder Dominik Adam. Die Fachabteilungen stellen die dafür erforderlichen Informationen zur Verfügung.

Der Betroffene ist spätestens innerhalb eines Monats über alle ergriffenen Massnahmen, die auf seinen Antrag hin erfolgt sind, zu informieren.

Der Datenschutzberater Patrick Ernst oder Dominik Adam steht bei der Wahrung der Betroffenenrechte beratend zur Verfügung.

Auskunfts- und Einsichtsrechte von Mitarbeitern werden durch Patrick Ernst oder Dominik Adam erfüllt.

XIV. Erhebung bzw. Verarbeitung von Personendaten

Die Erhebung und Verarbeitung Personendaten dürfen nur im Rahmen des rechtlich Zulässigen erfolgen. Hierbei sind auch die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäss Artikel 6 revDSG zu beachten. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.

Es wird sichergestellt, dass Betroffene keiner Entscheidung unterworfen werden, die ausschliesslich auf einer automatisierten Verarbeitung beruhen und zugleich den Betroffenen gegenüber einer rechtlichen Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (bspw. Profiling).

Vor Einführung neuer Arten von Erhebungen ist die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Hierbei sind insbesondere die vernünftigen Erwartungen des oder der Betroffenen hinsichtlich einer solchen Weiterverarbeitung gegen STARTNOW. SUPPORT AG die Art der verwendeten Daten, die Folgen für den Betroffenen sowie Möglichkeiten einer Verschlüsselung oder Pseudonymisierung zu prüfen. Die Prüfung ist darüber hinaus zu einem ordnungsgemässen Nachweis zu dokumentieren. Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person durch den Verantwortlichen eingeholt wird.

Gleichzeitig hat der für die Verarbeitung Verantwortliche vor der Erhebung bzw. der Speicherung von Daten schriftlich festzulegen, ob und in welcher Art und Weise der gesetzlichen Benachrichtigungspflicht des Betroffenen zu genügen ist.

Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse der Organisation besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der Datenschutzberater Patrick Ernst oder Dominik Adam kontaktieren.

XV. Datenhaltung, Versand, Löschung

Die Speicherung von Daten erfolgt grundsätzlich auf den hierzu zur Verfügung gestellten Netzlaufwerken. Eine Speicherung auf mobilen Datenträgern ist separat geregelt. Bei Netzwerken ist die IT-Abteilung für die Sicherung der Daten verantwortlich, die auf dem Server gespeichert sind.

Soweit technisch bedingt ein anderer Speicherort erforderlich ist (z.B. auf dem lokalen Laufwerk des Firmen-Computers) ist der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich.

Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten. Die IT-Abteilung ist über die Einhaltung der Termine insbesondere im Hinblick auf die Löschung von Personendaten in Sicherungskopien zu informieren.

Bei der Weiter- oder Rückgabe nicht mehr benötigter IT-Komponenten ist die IT-Abteilung verpflichtet, dafür zu sorgen, dass sämtliche Daten wirksam gelöscht werden.

XVI. Externe Dienstleister, Auftragsverarbeitung, Wartung

Sollen externe Dienstleister erstmals mit der Verarbeitung von Personendaten bzw. einzelnen Verarbeitungsschritten (z.B. Erhebung, Löschung = Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis von Personendaten bekommen, so ist Patrick Ernst oder Dominik Adam vor der Beauftragung unter Vorlage des den Anforderungen des Artikel 9 revDSG genügenden Vertragsentwurfs und der Kriterien der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren.

Entsprechendes gilt, falls die Organisation entsprechende Tätigkeiten im Auftrag Dritter wahrnehmen will.

XVII. Interne Mitteilungen

Massnahmen zur Sachverhaltsaufklärung und zur Vermeidung oder Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen im Arbeitsverhältnis sind unter genauer Beachtung der einschlägigen gesetzlichen Datenschutzvorschriften durchzuführen. Insbesondere muss die damit einhergehende Datenerhebung und -verwendung zum Erreichen des Ermittlungszwecks erforderlich, angemessen und mit Blick auf die schutzwürdigen Interessen des Betroffenen verhältnismässig sein.

Der Betroffene ist so bald wie möglich über die zu seiner Person durchgeführten Massnahmen zu informieren.

Bei allen Formen der internen Ermittlungen ist Patrick Ernst oder Dominik Adam hinsichtlich der Auswahl und Ausgestaltung der Massnahmen vorab einzubeziehen.

XVIII. Sicherheit der Verarbeitung

Für jedes Verfahren, welches sich nicht von Beginn an als frei von Risiken für den Betroffenen darstellt, ist in Abhängigkeit der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit eine dokumentierte Schutzbedarfsfeststellung sowie eine Analyse bzgl. der für den Betroffenen möglichen Risiken zu erstellen.

Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten sowie der Belastbarkeit der Daten verarbeitenden Systeme ist von der der IT-Abteilung ein allgemeines Sicherheitskonzept zu erstellen. Das Konzept orientiert sich an der zuvor erstellten Schutzbedarfsfeststellung und der Risikoanalyse. Dieses Konzept ist massgeblich für alle weiteren Verfahren. Das Sicherheitskonzept ist hinsichtlich der Wirksamkeit der dort vorgesehenen technisch-organisatorischen Massnahmen regelmässig zu überprüfen, zu bewerten und zu evaluieren.

XIX. Arbeitsanweisungen und Regelungen

Neben dieser Datenschutzleitlinie bestehen ergänzende Regelungen, die insbesondere die zur Realisierung des Datenschutzes und der Datensicherungsgebote zu treffende Massnahmen dienen.

XX. Rechenschafts- und Dokumentationspflicht

Die Einhaltung der Vorgaben, die sich aus dieser Leitlinie ergeben, muss jederzeit nachweisbar sein ("Accountability"). Eine Nachweisbarkeit hat insbesondere durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich getroffener Massnahmen und dazugehöriger Abwägungen zu erfolgen.

Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer und organisatorischer Veränderungen werden diese Richtlinie [und die dazugehörigen Arbeitsanweisungen und Regelungen] regelmässig auf Anpassungs- und Ergänzungsbedarf hin überprüft.

Änderungen dieser Richtlinie sind formlos wirksam. Die Beschäftigten und leitenden Angestellten sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.

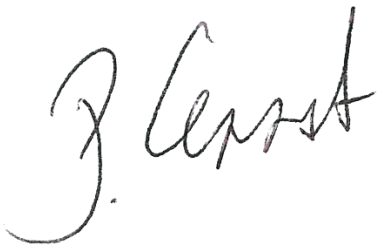
XXI. Kommunikation

Die Geschäftsführung stellt sicher, dass die Leitlinie allen Organisationsmitgliedern bekannt ist und beachtet wird.

XXII. Unterstützung durch die Geschäftsführung und Selbstverpflichtung

Die Einhaltung eines angemessenen Datenschutzniveaus erfordert personelle, finanzielle und zeitliche Ressourcen. Die Geschäftsführung erklärt, dass sie die Implementierung des Datenschutz-Managements sowie dessen kontinuierlicher Verbesserung mit geeigneten Mitteln unterstützen wird, damit die gesetzten Ziele sowie gesetzliche Datenschutzanforderungen erfüllt werden.

Horgen, 05.11.2023



Ort, Datum	Geschäftsführung Patrick Ernst

Horgen, 05.11.2023		
Ort, Datum		Geschäftsführung Dominik Adam