REISSWOLF Österreich GmbH

Datenschutz-Leitlinie

Verantwortung:	Informationssicherheitsbeauftragter
Klassifizierung:	Offen
Gültigkeitszeit:	Unbegrenzt
Überarbeitungsintervall:	Jährlich
Nächste Überarbeitung:	Mai 2024
Dateiname:	ISMS- Datenschutz-Leitlinie

Änderungs-Historie

Datum	Version	Änderung durch	Beschreibung der Änderung
02.05.2023	01	Manuel Moser	Übernahme ins ISMS

Freigabe

Datum	Version	Freigeben durch
02.05.2023	01	Thomas Rodrigo Beranek, MSc

Inhaltsverzeichnis

Vorwort

Lieber REISSWOLF-Mitarbeiter,

die Themen gesetzlicher Datenschutz und Informationssicherheit werden im Rahmen unserer Geschäftsbeziehungen immer wichtiger und bedeutsamer. Wir als Dienstleistungs- und Handelsunternehmen genießen ein hohes Vertrauen unserer Kunden und Lieferanten.

Vertrauen bedeutet jedoch auch Verantwortung für unser Handeln, für unsere Arbeit, für die Systeme und Daten der Mitarbeiter, Kunden und Partner. Unsere Geschäftspartner legen ihre persönlichen und betriebswirtschaftlichen Daten in unsere Hände und damit auch alle unternehmenswichtigen sowie kritischen Informationen.

Für uns als REISSWOLF ist es besonders wichtig, mit diesen Daten verantwortungsbewusst umzugehen. Daher liegt es sehr 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 zu verdeutlichen und auch den Mitarbeitern dieses Thema transparenter zu machen.

Thomas Rodrigo Beranek, MSc
Geschäftsführung REISSWOLF Österreich GmbH

1. Ziel der Datenschutz-Leitlinie

Die REISSWOLF Österreich GmbH verpflichtet sich im Rahmen ihrer gesellschaftlichen Verantwortung zur Einhaltung des gesetzlichen Datenschutzrechtes.

Diese Datenschutz-Leitlinie gilt für alle Unternehmensbereiche und Standorte der REISSWOLF Österreich GmbH und beruht auf akzeptierten Grundprinzipien zum Datenschutz.

Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen.

Wir definieren dazu ergänzend unsere eigenen Datenschutz-Ziele als Selbstverpflichtung.

Dazu gehören:

- Wir nehmen das Thema gesetzlicher Datenschutz ernst
- Wir machen Datenschutz zu einem Bestandteil unserer Unternehmenskultur
- Wir nehmen Betroffenenrechte ernst
- Wir nehmen das Thema Datenschutzverletzungen ernst
- Wir arbeiten nur mit Dienstleistern, die zu unserem Datenschutz-Konzept passen
- Wir nehmen die gesetzliche Informationspflicht ernst und arbeiten mit der notwendigen Transparenz
- Wir sehen Datenschutz als Chance, bestehende Prozesse zu überarbeiten
- Wir alle arbeiten bei der Einhaltung der Vorgaben aktiv mit und verbessern uns kontinuierlich

1.1 Zuständigkeiten

Datenschutz-Ziel	Zuständigkeit
Datenschutz-Vorgaben	Thomas Rodrigo Beranek, MSc
Datenschutz als Unternehmenskultur	Thomas Rodrigo Beranek, MSc
Datenschutz als Chance zur Prozessverbesserung	Manuel Moser
Betroffenenrechte	Manuel Moser
Datenschutzverletzungen	Manuel Moser
Auftragsverarbeiter	Mag. Werner Gruber
Informationspflicht/Transparenz	Manuel Moser
Einhaltung der Vorgaben (int. DS-Controlling)	Manuel Moser
Datenschutz-Folgenabschätzung	Manuel Moser
Datenschutz-Schulungen	Manuel Moser
Datenschutz-Koordinator (DSK)	Manuel Moser
Datenschutz-Beauftragter (DSBA) (extern)	Ronald Kopecky

2. Geltungsbereich und Änderung der Datenschutz-Leitlinie

Diese Datenschutz-Leitlinie basiert auf den Vorgaben der EU-Datenschutz-Grundverordnung (EU 2016/679) und den dazugehörigen nationalen Gesetzen.

Die aktuelle Version der REISSWOLF Datenschutz-Leitlinie kann auf der Internetseite der REISSWOLF Österreich GmbH (www.reisswolf.at) abgerufen werden.

3. Was sind personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die eine natürliche oder juristische Person identifizieren (in Österreich gilt die Erweiterung auf die juristische Person).

Die Identifizierbarkeit kann direkt, indirekt oder mittels Zuordnung sein, sowie alle Zuordnungen zu einem oder mehrerer besonderer Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen oder juristischen Person sind.

Beispiele für personenbezogene Daten sind:

- Name (z.B. Max Mustermann) – direkte Identifizierbarkeit
- „Der Geschäftsführer von REISSWOLF" – indirekte Identifizierbarkeit
- Adresse
- Geburtsdatum
- Bankdaten
- IP-Adressen
- Kennnummern, Online-Kennungen, Kennzeichen
- Standortdaten
- Fingerabdrücke, Irisdaten (biometrische Daten)
- uvm.

4. Was bedeutet Verarbeitung

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

Unter Löschen oder Vernichtung wird die Unwiederbringlichkeit verstanden.

5. Prinzipien für die Verarbeitung personenbezogener Daten

5.1 Fairness und Rechtmäßigkeit

Bei der Verarbeitung personenbezogener Daten muss das informationelle Selbstbestimmungsrecht des Betroffenen gewahrt werden. Das bedeutet, dass der Dateneigentümer darüber bestimmen darf, was mit den ihn betreffenden personenbezogenen Daten passiert.

Personenbezogene Daten müssen auf rechtmäßige Weise erhoben und verarbeitet werden. Rechtmäßigkeit bedeutet:

- die Verarbeitung wurde durch den Dateneigentümer genehmigt
- die Verarbeitung dient einer Vertragserfüllung oder einer vorvertraglichen Maßnahme
- die Verarbeitung erfolgt aufgrund einer rechtlichen Verpflichtung
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen zu schützen
- die Verarbeitung dient dem öffentlichen Interesse
- die Verarbeitung dient der Wahrung berechtigter Interessen von REISSWOLF Österreich

5.2 Zweckbindung

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Zwecke müssen zum Zeitpunkt der Datenerhebung dem Dateneigentümer mitgeteilt werden.

Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung sowie einer neuerlichen Genehmigung durch den Dateneigentümer.

5.3 Transparenz

Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:

- die Identität der verantwortlichen Stelle (REISSWOLF Österreich GmbH)
- den Zweck der Datenverarbeitung (z.B. Kunden-Stammdatenanlage, etc.)
- die hinterlegten Aufbewahrungsfristen
- Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden (z.B. Professionisten, etc.)

5.4 Datenvermeidung und Datensparsamkeit

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

Personenbezogene Daten dürfen nicht auf Vorrat für potenzielle, zukünftige Zwecke gespeichert werden.

5.5 Löschung und Speicherbegrenzung

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen proaktiv gelöscht werden.

5.6 Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten sind richtig, vollständig und – soweit möglich – 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.

5.7 Vertraulichkeit und Datensicherheit

Für personenbezogene Daten gilt das Datengeheimnis.

Sie müssen durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

Es ist dafür zu sorgen, dass durch die Verarbeitung personenbezogener Daten den Dateneigentümern kein Schaden zugefügt wird.

6. Zulässigkeit der Datenverarbeitung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

6.1 Kunden-, Lieferanten- oder Partnerdaten

6.1.1 Datenverarbeitung für eine vertragliche Beziehung

Wenn die Datenverarbeitung personenbezogener Daten der Vertragserfüllung oder der Erfüllung vorvertraglicher Maßnahmen dient, so ist die Verarbeitung zulässig.

6.1.2 Datenverarbeitung zu Werbezwecken

Wendet sich der Betroffene mit einem Informationsanliegen an REISSWOLF Österreich (z.B. Wunsch nach Zusendung von einem Produktkatalog), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig. Für weitere Kundenbindungs- oder Werbemaßnahmen gilt die Einwilligung in die Datenverarbeitung (siehe 6.1.3).

6.1.3 Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Die Erteilung muss dokumentiert werden.

6.1.4 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten.

6.1.5 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der REISSWOLF Österreich GmbH erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z.B. Vermeidung von Vertragsstörungen).

6.1.6 Verarbeitung besonders schutzwürdiger Daten (Daten besonderer Kategorien)

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat.

Daten besonderer Kategorien sind:

- Informationen zur rassischen und ethnischen Herkunft
- Informationen zu politischen Meinungen
- Informationen zu religiösen oder weltanschaulichen Überzeugungen
- Informationen, aus denen die Gewerkschaftszugehörigkeit hervorgeht
- genetische und biometrische Daten
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung

Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen.

6.1.7 Automatisierte Einzelentscheidungen (Profiling)

Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (z.B. Kreditwürdigkeit) bewertet werden, dürfen nicht die ausschließliche Grundlage für Entscheidungen mit negativen rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen sein.

Dem Betroffenen muss die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit zu einer Stellungnahme gegeben werden. Zur Vermeidung von Fehlentscheidungen muss eine Kontrolle und eine Plausibilitätsprüfung durch einen Mitarbeiter gewährleistet werden.

Automatisierte Einzelentscheidungen (Profiling) werden bei REISSWOLF Österreich aktuell nicht durchgeführt.

6.1.8 Homepage-Nutzerdaten und Internet

Wenn auf Webseiten oder in Apps personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzerklärungen und ggf. Cookie- Hinweisen zu informieren. Die Datenschutzhinweise und ggf. Cookie-Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind.

Werden zur Auswertung des Nutzungsverhaltens von Webseiten und Apps Nutzungsprofile erstellt (Tracking), so müssen die Betroffenen darüber in jedem Fall in den Datenschutzerklärungen informiert werden. Erfolgt das Tracking unter einem Pseudonym, so soll dem Betroffenen in den Datenschutzerklärungen eine Widerspruchsmöglichkeit eröffnet werden (Opt-Out).

6.2 Mitarbeiterdaten

6.2.1 Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind.

Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt. Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren oder vor der Weitergabe der Bewerbung an andere Unternehmensteile erforderlich.

Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift.

Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich, ist eine Einwilligung des Betroffenen einzuholen.

Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

6.2.2 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Mitarbeiterdaten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden.

6.2.3 Kollektivregelungen für Datenverarbeitungen

Geht eine Verarbeitung über den Zweck der Vertragsabwicklung hinaus, so ist sie auch dann zulässig, wenn sie durch eine Kollektivregelung gestattet wird. Kollektivregelungen sind z.B. Vereinbarungen zwischen Arbeitgeber und Arbeitnehmervertretungen im Rahmen der Möglichkeiten des jeweiligen Arbeitsrechts.

Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen des staatlichen Datenschutzrechts gestaltbar.

6.2.4 Einwilligung in die Datenverarbeitung

Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung des Betroffenen stattfinden.

Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung muss in jedem Fall ordnungsgemäß dokumentiert werden. Bei einer freiwilligen Angabe von Daten durch den Betroffenen kann eine Einwilligung angenommen werden, wenn nationales Recht keine explizite Einwilligung vorschreibt. Vor der Einwilligung muss der Betroffene gemäß dieser Datenschutz-Leitlinie informiert werden.

6.2.5 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der REISSWOLF Österreich GmbH erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z.B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlich begründet.

Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen. Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen.

Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden.

Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahme (z.B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechtigte Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Maßnahme festgestellt und dokumentiert werden.

Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen (z.B. Mitbestimmungsrechte der Arbeitnehmervertretung und Informationsrechte der Betroffenen) berücksichtigt werden.

6.2.6 Verarbeitung besonders schutzwürdiger Daten (Daten besonderer Kategorien)

Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden.

Daten besonderer Kategorien sind:

- Informationen zur rassischen und ethnischen Herkunft
- Informationen zu politischen Meinungen
- Informationen zu religiösen oder weltanschaulichen Überzeugungen
- Informationen, aus denen die Gewerkschaftszugehörigkeit hervorgeht
- genetische und biometrische Daten
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung

Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden.

Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann. Der Mitarbeiter kann freiwillig als auch ausdrücklich in die Verarbeitung einwilligen.

6.2.7 Automatisierte Entscheidungen (Profiling)

Soweit im Beschäftigungsverhältnis personenbezogene Daten automatisiert verarbeitet werden, durch die einzelne Persönlichkeitsmerkmale bewertet werden (z.B. im Rahmen der Personalauswahl oder der Auswertung von Fähigkeitsprofilen), darf eine solche automatisierte Verarbeitung nicht die ausschließliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für die betroffenen Mitarbeiter sein.

Um Fehlentscheidungen zu vermeiden, muss in automatisierten Verfahren gewährleistet sein, dass eine inhaltliche Bewertung des Sachverhalts durch eine natürliche Person erfolgt und diese Bewertung Grundlage für die Entscheidung ist.

Dem betroffenen Mitarbeiter muss außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden.

Automatisierte Einzelentscheidungen (Profiling) werden bei REISSWOLF Österreich aktuell nicht durchgeführt.

6.2.8 Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, Intranet und Internet sowie interne soziale Netzwerke werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der geltenden unternehmensinternen Richtlinien genutzt werden.

Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Intranet- und Internet-Nutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer sind Schutzmaßnahmen an den Übergängen in das REISSWOLF-Netzwerk implementiert worden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit und Nachvollziehbarkeit wird die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und Internets sowie der internen sozialen Netzwerke protokolliert.

Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten und begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien der REISSWOLF Österreich GmbH erfolgen. Diese Kontrollen dürfen nur unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen. Die jeweiligen nationalen Gesetze sind ebenso zu beachten wie die hierzu bestehenden Unternehmensregeln. Die Auswertungen dienen nicht der Leistungserfassung.

7. Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb der REISSWOLF Österreich GmbH oder an Empfänger innerhalb der REISSWOLF Österreich GmbH unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten.

Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden. Die Verpflichtung hat schriftlich zu erfolgen und hat folgende Punkte zu beinhalten:

- Definition der Zwecke der Verarbeitung
- Gewährleistung des ausschließlichen Einsatzes von Personal, welches zur Vertraulichkeit und Geheimhaltung verpflichtet wurde
- Gewährleistung der angemessenen Sicherheit gem. Art. 32 DSGVO
- Regelung für Sub-Auftragsverarbeiter
- Verpflichtung zur Einhaltung der Betroffenenrechte
- Datenlöschung oder Rückgabe nach Auftragserfüllung
- Kontrollrecht durch REISSWOLF Österreich oder einen durch REISSWOLF Österreich beauftragten Prüfer

Im Falle einer Datenübermittlung an einen Empfänger außerhalb der REISSWOLF Österreich GmbH in einem Drittstaat, muss dieser ein zu dieser Datenschutz-Leitlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt. Eine solche Übermittlung findet aktuell nicht statt.

Im Falle einer Datenübermittlung von Dritten an die REISSWOLF Österreich GmbH muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

8. Auftragsverarbeitung (Dienstleister)

Eine Auftragsverarbeitung liegt vor, wenn ein Auftragnehmer (z.B. Auftragsverarbeiter oder Dienstleister) mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. In diesen Fällen ist mit externen Auftragnehmern eine Vereinbarung über eine Auftragsverarbeitung abzuschließen.

Dabei behält die REISSWOLF Österreich GmbH die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen der REISSWOLF Österreich GmbH verarbeiten. Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten; der beauftragende Fachbereich muss ihre Umsetzung sicherstellen.

1. Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.
2. Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten der REISSWOLF Österreich GmbH und des Auftragnehmers zu dokumentieren.
3. Die REISSWOLF Österreich GmbH hat sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers zu überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung (z.B. ISO 27001) nachweisen. Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmäßig zu wiederholen.
4. Bei einer grenzüberschreitenden Auftragsverarbeitung sind die jeweiligen nationalen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland zu erfüllen. Insbesondere darf die Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum in einem Drittstaat nur stattfinden, wenn der Auftragnehmer ein zu dieser Datenschutz-Leitlinie gleichwertiges Datenschutzniveau nachweist.
5. Anerkennung verbindlicher Unternehmensregeln des Auftragnehmers zur Schaffung eines angemessenen Datenschutzniveaus durch die zuständigen Datenschutz-Aufsichtsbehörden.

9. Rechte des Betroffenen

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.

1. Der Betroffene kann **Auskunft** darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind. Falls im Arbeitsverhältnis nach dem jeweiligen Arbeitsrecht weitergehende Einsichtsrechte in Unterlagen des Arbeitgebers (z.B. Personalakte) vorgesehen sind, so bleiben diese unberührt.
2. Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.
3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre **Berichtigung oder Ergänzung** verlangen.
4. Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung **widersprechen**. Für diese Zwecke müssen die Daten gesperrt werden.
5. Der Betroffene ist berechtigt, die **Löschung** seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.
6. Der Betroffene hat ein grundsätzliches **Widerspruchsrecht** gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

Im Falle des Eintreffens eines Betroffenenrechts ist unverzüglich der Zuständige für Betroffenenrechte - siehe Punkt 1.1 Tabelle der Zuständigkeiten - per E-Mail in vollem Umfang zu informieren.

10. Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte oder unrechtmäßige 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 und entsprechend berechtigt zu sein. Es gilt das Need-to-know-Prinzip: Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.

Es ist den Mitarbeitern untersagt, personenbezogene Daten für eigene private oder wirtschaftliche Zwecke zu nutzen, an Unbefugte zu übermitteln oder diese auf andere Weise zugänglich zu machen.

11. Offenlegung von personenbezogenen Daten

Es ist den Mitarbeitern untersagt, personenbezogene Daten Dritten gegenüber offenzulegen, es sei denn, die Offenlegung entspricht den Zulässigkeitskritierien gem. Pkt. 5 bis 10 dieser Leitlinie.

Im Falle einer Anfrage zur Offenlegung (Gerichte, Polizei, etc.), ist der Datenschutz-Koordinator per E-Mail in vollem Umfang zu informieren. Eine Offenlegung ist ausschließlich durch die Geschäftsführung freizugeben.

12. Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen.

Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten (ermittelt durch den Prozess zur Informationsklassifizierung) zu orientieren.

Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des unternehmensweiten Informationssicherheits- und Datenschutz-Managements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

Es ist den Mitarbeitern untersagt, personenbezogene Daten außerhalb der von REISSWOLF Österreich zur Verfügung gestellten Services (Programme, Ablagen, etc.) und Prozesse sowie außerhalb nachvollziehbarer und rechtmäßiger Aufträge zu verarbeiten.

13. Datenschutz-Folgenabschätzung

Soll eine neue Form einer Verarbeitung (siehe Punkt 4) personenbezogener Daten eingeführt werden oder ist geplant, eine bestehende Verarbeitung personenbezogener Daten zu verändern, so ist der Datenschutz-Koordinator (siehe Punkt 1.1 Tabelle der Zuständigkeiten) vorab per E-Mail in vollem Umfang zu informieren.

Eine neue Verarbeitung sowie eine geplante Veränderung einer bestehenden Verarbeitung benötigen eine Vorab-Freigabe durch den Datenschutz-Koordinator. Bis zur Vorlage dieser Freigabe ist es den Mitarbeitern untersagt, neue Verarbeitungen bzw. Veränderungen an bestehenden Verarbeitungen durchzuführen.

14. Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch interne und externe Datenschutzaudits und weitere Kontrollen überprüft.

15. Datenschutzvorfälle (Datenschutzverletzungen)

Jeder Mitarbeiter muss der Geschäftsführung unverzüglich Fälle von Verstößen gegen diese Datenschutz-Leitlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle) melden.

In Fällen von

- unbefugter oder unrechtmäßiger Verarbeitung
- unbeabsichtigter oder unrechtmäßiger Vernichtung
- unbeabsichtigtem oder unrechtmäßigem Verlust
- unbeabsichtigter oder unrechtmäßiger Veränderung
- unbeabsichtigter oder unrechtmäßiger Offenlegung

ist unverzüglich die dafür zuständige Person – siehe Punkt 1.1 Zuständigkeiten – per E-Mail in vollem Umfang zu informieren, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.

16. Verantwortlichkeiten und Sanktionen

Die Geschäftsführung ist für die verordnungskonforme Datenverarbeitung personenbezogener Daten verantwortlich.

Damit ist sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutz-Leitlinie enthaltenen Anforderungen des Datenschutzes eingehalten werden (z.B. nationale Meldepflichten).

Es ist eine Managementaufgabe der Geschäftsführung, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen. Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter.

Die Geschäftsführung stellt sicher, dass ihre Mitarbeiter im erforderlichen Umfang zum Datenschutz geschult werden.

Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

17. Der Datenschutz-Koordinator / Datenschutz-Beauftragte

Der Datenschutz-Koordinator (DSK) als internes Organ bzw. der externe Datenschutz-Beauftragte (DSBA) wirkt auf die Einhaltung der Datenschutzvorschriften hin.

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Datenschutz-Koordinator wenden. Anfragen und Beschwerden werden natürlich streng vertraulich behandelt.

17.1 Der Datenschutz-Beauftragte

Der externe Datenschutz-Beauftragte erfüllt seine Pflichten gemäß den im Vertrag definierten Aufgaben und der gesetzlichen Vorgaben gem. Art. 39 DSGVO.

Herr Ronald Kopecky
KOMDAT Datenschutz GmbH
Linzer Straße 60
4614 Marchtrenk
+43 7243 54300
www.komdat.at
office@komdat.at

18. Inkraftsetzung

Dieses Dokument wird einmal jährlich sowie bei Bedarf auf Vollständigkeit und Aktualität überprüft.

Änderungen dieses Dokuments liegen in der Verantwortung des Zuständigen für Datenschutz-Vorgaben.

Dieses Dokument ist allen Mitarbeitern zugänglich zu halten.

Thomas Rodrigo Beranek, MSc
Geschäftsführung REISSWOLF Österreich GmbH