Leitlinie zum Datenschutz

Version 2017

ARAG KONZERN

Dokumentinformationen

Dokument:	Leitlinie zum Datenschutz
Letzte Version:	1.0
Datum:	01.12.2017
Autor(en):	Projekt EU Datenschutzgrundverordnung
Ansprechpartner:	Datenschutzbeauftragter

Abnahmehistorie

Version	Datum	Name / Organ
1.0	Nov 2017	Zustimmend zu Kenntnis genommen: Hauptabteilungsleiter der Hauptabteilungen Recht/Compliance, Konzern Risikomanagement und Konzern Revision Datenschutzbeauftragter und IT-Sicherheitsbeauftragter
	05.12.2017	Vorstand ARAG SE
	12.12.2017	Lenkungsausschuss Projekt EU Datenschutzgrundverordnung
	14.12.2017	Vorstand der ARAG Holding SE
	15.12.2017	Vorstand der ARAG Allgemeine Versicherungs-AG
	15.12.2017	Vorstand der Interlloyd Versicherungs-AG
	24.01.2018	Vorstand der ARAG Krankenversicherungs-AG

Inhaltsverzeichnis

1 Unser Anspruch

Als international tätiger Versicherungskonzern messen wir dem Schutz und der Sicherheit von personenbezogenen Daten höchste Bedeutung zu. Die Achtung der Persönlichkeitsrechte ist für uns die Basis für eine vertrauensvolle Zusammenarbeit mit Kunden, Partnern und Mitarbeitern.

Unser Anspruch ist es, dass die Unternehmen des ARAG-Konzerns nicht nur für ausgezeichneten Versicherungsschutz stehen, sondern in Zeiten der Digitalisierung auch führend bei der Wahrung der Privatsphäre ist. Es ist daher für uns selbstverständlich, den gesetzlichen Vorgaben bei der Erhebung und Verarbeitung personenbezogener Daten gerecht zu werden. Dazu zählen insbesondere die Regelungen der EU Datenschutzgrundverordnung sowie alle anwendbaren Datenschutzvorschriften.

Die vorliegende Leitlinie zum Datenschutz beschreibt die Grundsätze und Maßnahmen zum Schutz der Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung ihrer personenbezogenen Daten. Diese gelten für alle Gesellschaften des ARAG-Konzerns, die diese Leitlinie in Kraft gesetzt haben.

2 Unsere Grundsätze für die Datenverarbeitung

Bei der Verarbeitung von personenbezogenen Daten werden von uns die nachfolgenden Grundsätze zugrunde gelegt:

- **Rechtmäßigkeit**: Für die Verarbeitung von personenbezogenen Daten bedarf es stets einer rechtlichen Grundlage.
- **Transparenz**: Jeder Betroffene muss die Verarbeitung seiner personenbezogenen Daten nachvollziehen können.
- **Zweckbindung**: Die Zwecke, zu denen personenbezogene Daten verarbeitet werden, sind vorab eindeutig zu benennen und zum Zeitpunkt der Erhebung festzulegen.
- **Datenminimierung**: Die Verarbeitung von personenbezogenen Daten ist auf das für den Zweck der Verarbeitung angemessene, sachliche, relevante und notwendige Maß zu beschränken. Entsprechendes gilt für Zugriffsmöglichkeiten.
- **Richtigkeit**: Personenbezogene Daten sind richtig und vollständig zu speichern bzw. zu verarbeiten und aktuell zu halten. Entsprechend werden angemessene Maßnahmen getroffen, um nicht zutreffende, unvollständige oder veraltete Daten zu löschen, zu berichtigen, zu ergänzen oder zu aktualisieren.
- **Speicherbegrenzung**: Personenbezogene Daten dürfen nur solange gespeichert werden, wie es für die Verarbeitungszwecke erforderlich bzw. aufgrund anderweitiger

gesetzlicher Vorgaben zulässig ist (z.B. handels-/steuerrechtliche Aufbewahrungspflichten).

- **Integrität und Vertraulichkeit**: Für die Verarbeitung von personenbezogenen Daten sind geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten, insbesondere vor unbefugter oder unrechtmäßiger Verarbeitung, zufälligem Verlust, zufälliger Zerstörung oder Schädigung zu ergreifen.

Für uns ist es im Sinne einer bewussten Wahrnehmung unserer Verantwortung selbstverständlich, die Verarbeitung von personenbezogenen Daten zum Nachweis der oben genannten Grundsätze zu dokumentieren.

3 Zulässigkeit der Datenverarbeitung

Jede Verarbeitung von personenbezogenen Daten unterliegt dem Prinzip des „**Verbots mit Erlaubnisvorbehalt**“. Demnach ist die Verarbeitung von personenbezogenen Daten unzulässig, wenn keine Rechtsgrundlage dafür besteht. In den Gesellschaften des ARAG-Konzerns werden personenbezogene Daten insbesondere aus folgenden Gründen (zulässigerweise) verarbeitet:

- **Erfüllung oder Vorbereitung eines Vertrages**, z.B. Verarbeitung von Anschriftendaten zwecks postalischer Kommunikation.
- **Erfüllung einer rechtlichen Verpflichtung**, z.B. Speicherung von Dokumenten nach finanz-/handelsrechtlichen Aufbewahrungspflichten.
- **Berechtigte Interessen**, z.B. postalische Eigenwerbung (sofern kein Widerspruch vorliegt).
- **Einwilligung des Betroffenen**, z.B. zur telefonischen Kontaktaufnahme oder Verarbeitung von Gesundheitsdaten.

Besondere Kategorien von personenbezogenen Daten, z.B. zur ethnischen Herkunft oder religiösen Überzeugungen oder in Bezug auf die Gesundheit dürfen nur aufgrund einer ausdrücklichen Einwilligung oder gesetzlichen Erlaubnis verarbeitet werden.

4 Betroffenenrechte

Die Wahrung der Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten hat in den Gesellschaften des ARAG-Konzerns höchste Priorität. Um dies zu gewährleisten stehen dem Betroffenen u.a. die folgenden Rechte zu:

- **Information**: Betroffene werden frühzeitig und transparent darüber informiert, ob und wie deren Daten verarbeitet werden. Das gilt sowohl für den Fall, dass personenbezogene

Daten beim Betroffenen direkt erhoben werden als auch für die Erhebung bei anderen Stellen (Dritterhebung).

- **Auskunft**: Betroffene können jederzeit Auskunft über die von ihnen gespeicherten und/oder verarbeiteten personenbezogenen Daten sowie eine Kopie der gespeicherten und/oder verarbeiteten personenbezogenen Daten verlangen.
- **Berichtigung und Vervollständigung**: Betroffene können jederzeit die Berichtigung oder Vervollständigung von falschen oder unvollständigen personenbezogenen Daten verlangen, z.B. wenn ein Name oder eine Adresse fehlerhaft ist.
- **Löschung**: Betroffene können die Löschung ihrer personenbezogenen Daten verlangen, soweit keine entgegenstehenden Pflichten oder Rechte bestehen, z.B. steuer-/handelsrechtliche Aufbewahrungspflichten. Der Betroffene hat zudem ein Recht auf „Vergessenwerden“ mit der Folge, dass andere Verantwortliche über das Löschbegehren informiert werden, sofern diesen gegenüber personenbezogene Daten durch die ARAG offengelegt wurden.
- **Einschränkung der Verarbeitung**: Betroffene können die Einschränkung der Verarbeitung ihrer personenbezogenen Daten verlangen, z.B. wenn diese fehlerhaft sind.
- **Widerspruch**: Betroffene können der Verarbeitung ihrer personenbezogenen Daten zu Werbezwecken jederzeit widersprechen. Ansonsten ist ein Widerspruch unter bestimmten Voraussetzungen aufgrund besonderer persönlicher Umstände des Betroffenen möglich.
- **Automatisierte Einzelfallentscheidung**: Betroffene unterliegen im Rahmen einer effizienten Geschäftsabwicklung nur dann einer automatisierten Einzelfallentscheidung, sofern dies zulässig ist, z.B. im Rahmen der Vertragserfüllung. Betroffene werden dabei über entsprechende automatisierte Verarbeitungsvorgänge informiert.

Dem Betroffenen werden sämtliche Informationen im Hinblick auf die Verarbeitung seiner personenbezogenen Daten leicht zugänglich und in einer klaren und einfachen Sprache mitgeteilt.

Sollte es zu einer Verletzung des Schutzes personenbezogener Daten kommen, werden Betroffene bei Vorliegen der rechtlichen Voraussetzungen im Hinblick auf Risiken für ihre Rechte und Freiheiten über solche Ereignisse informiert.

Dem Betroffenen steht es frei, sich beim Unternehmen zu beschweren, sich an den zuständigen Datenschutzbeauftragten, die Datenschutz-Aufsichtsbehörde oder ein Gericht zu wenden, um seine Rechte und Freiheiten bei der Verarbeitung von personenbezogenen Daten wahrzunehmen. Gesetzliche Rechte und Ansprüche von Betroffenen bleiben unberührt.

5 Auftragsverarbeitung & Datenübermittlung

Werden personenbezogene Daten durch externe Dienstleister oder Partner im Auftrag der ARAG verarbeitet, werden – je nach Konstellation – geeignete datenschutzrechtliche Sicherungsmaßnahmen für die Verarbeitung ergriffen, z.B:

- **Auftragsverarbeitung**: Verarbeitet der Dienstleister personenbezogene Daten auf Weisung, werden zur Absicherung Vereinbarungen zur Auftragsverarbeitung mit dem Dienstleister abgeschlossen und nur solche Dienstleister beauftragt, die zum Schutz angemessene technische und organisatorische Maßnahmen ergreifen. Gleiches gilt für den Fall des Datenzugriffs im Rahmen von Service- und Wartungsleistungen.
- **Funktionsübertragung**: Wird ein Externer über die Verarbeitung von personenbezogenen Daten hinaus mit weiteren Aufgaben betraut, für deren Ausübung er eine eigene Entscheidungsbefugnis bzgl. der Datenverwendung benötigt, so werden – vergleichbar der Auftragsverarbeitung – datenschutzrechtliche Vereinbarungen mit diesem abgeschlossen, die angemessene technische und organisatorische Maßnahmen vorsehen.
- **Vertraulichkeitsvereinbarung**: Kann im Einzelfall nicht ausgeschlossen werden, dass in einem eingeschränkten Umfang personenbezogene Daten offengelegt werden (müssen), so erfolgt zur Absicherung der Abschluss einer Vertraulichkeitsvereinbarung.

Werden personenbezogene Daten außerhalb der EU verarbeitet bzw. können diese von dort eingesehen werden, erfolgt dies nur, sofern geeignete Garantien und Nachweise zur Sicherheit der Verarbeitung existieren, z.B. durch Abschluss von Standard Datenschutzklauseln.

6 Datensicherheit, Folgenabschätzung und Technikgestaltung

Zum Schutz der Verarbeitung von personenbezogenen Daten werden von uns angemessene **technische und organisatorische Maßnahmen** ergriffen. Dazu zählen insbesondere Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten einschließlich der Belastbarkeit von Systemen und Diensten.

Bei sämtlichen Verarbeitungsvorgängen werden für die Auswahl von technischen und organisatorischen Maßnahmen die **Risiken** für die Rechte und Freiheiten von Betroffenen berücksichtigt. Im Fall von hohen Risiken durchlaufen die Verarbeitungsvorgänge eine zusätzliche Risiko- und Maßnahmenprüfung.

Bei der Verarbeitung von personenbezogenen Daten wird der Grundsatz „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“ beachtet, z.B. durch die **Pseudonymisierung** oder die **Minimierung** von personenbezogenen Daten.

Technische und organisatorische Maßnahmen werden regelmäßig im Hinblick auf ihre Wirksamkeit geprüft und nach Bedarf unter Berücksichtigung des Stands der Technik angepasst. Dies gilt auch für die technischen und organisatorischen Maßnahmen beim Einsatz von externen Dienstleistern oder Partnern.

7 Verantwortlichkeiten und Datenschutzorganisation

Für die Umsetzung der datenschutzrechtlichen Vorgaben ist die jeweilige Gesellschaft des ARAG-Konzerns verantwortlich. Dort schafft die Unternehmensleitung als verantwortliche Stelle die notwendigen Voraussetzungen zur Umsetzung der datenschutzrechtlichen Vorgaben durch die Mitarbeiter/innen der Fachabteilungen. Dies gilt auch für Niederlassungen der Gesellschaft außerhalb ihres Sitzlands.

Unterstützt wird die betriebliche Umsetzung und Einhaltung der Datenschutzvorgaben durch den Konzerndatenschutzbeauftragten und einer dezentralen Datenschutzorganisation einschließlich internationaler Datenschutzverantwortlichen, mittels derer die Anforderungen international sichergestellt werden.

Die Grundlagen und Ausprägungen des Datenschutz Management Systems im ARAG-Konzern werden in der ergänzenden Datenschutzmanagement Richtlinie umfassend beschrieben.

Über die in dieser Leitlinie genannten Vorgaben hinaus gelten – je nach Geschäftstätigkeit der jeweiligen Gesellschaft – ergänzende Datenschutzanforderungen, in Deutschland z.B. die Selbstverpflichtung gemäß „Verhaltensregeln für den Umgang mit personenbezogenen Daten der deutschen Versicherungswirtschaft“ (Code of Conduct). Die Leitlinie zum Datenschutz wird als Konzernleitlinie vom jeweiligen Gesamtvorstand der jeweiligen Gesellschaft verabschiedet. Sie wird jährlich durch den betrieblichen Datenschutzbeauftragten auf Aktualität überprüft und bei wesentlichen Änderungen vom Gesamtvorstand erneut verabschiedet.