Datenschutzrichtlinie

Dokumenteninformationen			
Klassifikation:	intern		
Versionsnummer:	2.0		
Dokumententitel:	Datenschutzrichtlinie		
Dokumentenverantwortlicher:	Marvin Schmidtmer		
Erstellt am:	16.03.2020	Erstellt von:	Marvin Schmidtmer
		Funktion des Erstellers:	ISO
Letzte Überarbeitung:	30.03.2020	Nächste Überarbeitung:	-
Freigabe am:	18.03.2020	Freigabe von:	Marius Jäger

Versionsverlauf			
Datum	Version	Beschreibung	verändert durch
02.04.2020	2.0	Neue Version in Windream erstellt; Anpassung an CI; Dokumenteninformationen hinzugefügt; ergänzte Kapitel: Verarbeitungsverzeichnis, Datengeheimnis; Änderung Jäger Gruppe zu Jäger Group; formelle Anpassungen	Marvin Schmidtmer

Mitgeltende Dokumente:
IT-Richtlinie
Technisch organisatorische Maßnahmen (TOM)
Verarbeitungsverzeichnis

1. Inhaltsverzeichnis

Inhalt

2. Vorwort

Liebe Mitarbeiter der Jäger Group,

die Themen gesetzlicher Datenschutz und Informationssicherheit werden für uns und unsere Geschäftspartner immer bedeutsamer.

Dies bedeutet Verantwortung für unser Handeln, für unsere Arbeit, für die Systeme und Daten unserer Geschäftspartner zu übernehmen.

In der Jäger Group ist es uns besonders wichtig, mit personenbezogenen 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 Richtlinie soll helfen, die Bedeutung und Wichtigkeit des gesetzlichen Datenschutzes zu verstehen und auch Ihnen dieses Thema nahe zu bringen.

Marius-Quintus Jäger Sebastian Jäger Dr. Andreas Jäger

Zuständigkeiten

Datenschutzmanagement:	Marvin Schmidtmer
Auftragsverarbeitung:	Marvin Schmidtmer
Betroffenenrechte:	Marvin Schmidtmer
Datenschutzverletzungen:	Marvin Schmidtmer
Technische Sicherheit:	Marvin Schmidtmer
Verfahrensverzeichnis:	Marvin Schmidtmer
Datenschutzbeauftragte/r:	Arnold Jäger Holding GmbH SRAin Isabel Müller-Wilckens Telefon 0511-5358-218 E-Mail: dataprotection@jaegergruppe.de

3. Ziel der Datenschutzrichtlinie

Die Jäger Group verpflichtet sich zur Einhaltung der geltenden Datenschutzbestimmungen und schafft damit die Grundlage für eine vertrauensvolle Zusammenarbeit mit Mitarbeitern und Geschäftspartnern.

Dies stärkt den Anspruch der Jäger Group, in einer sich rasch ändernden, informationstechnischen Gesellschaft ein zuverlässiger und zukunftsfähiger Geschäftspartner sowie ein attraktiver Arbeitgeber zu sein.

Das Datenschutzkonzept hat zum Ziel, in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte darzustellen. Es kann auch als Grundlage für datenschutzrechtliche Prüfungen z. B. durch Auftraggeber im Rahmen der Auftragsverarbeitung genutzt werden. Dadurch soll die Einhaltung der europäischen Datenschutzgrundverordnung (DSGVO) nicht nur gewährleistet, sondern auch der Nachweis der Einhaltung geschaffen werden.

4. Geltungsbereich

Diese Datenschutzrichtlinie ergibt sich aus den Vorgaben der EU-Datenschutzgrundverordnung und den dazugehörigen nationalen Gesetzen. In Bezug auf die technische Sicherheit orientiert sie sich an der DIN ISO/IEC 27001:2017.

Diese Datenschutzrichtlinie gilt für die gesamte Jäger Group und beruht auf normierten Grundprinzipien zum Datenschutz und zur Datensicherheit.

Die Datenschutzrichtlinie in ihrer jeweils aktuellen Fassung kann im Intranet der Jäger Group abgerufen werden.

5. Begriffe und Abkürzungen

AJH	Arnold Jäger Holding GmbH
DSB	Datenschutzbeauftragte/r
TOM	technisch organisatorische Maßnahmen
Windream BPM Client	Software zur Darstellung und Bearbeitung von Workflows

6. Prinzipien für die Verarbeitung personenbezogener Daten

Fairness und Rechtmäßigkeit

Bei der Verarbeitung personenbezogener Daten muss das informationelle Selbstbestimmungsrecht des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise erhoben und verarbeitet werden.

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.

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
- den Zweck der Datenverarbeitung
- die hinterlegten Aufbewahrungsfristen
- Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

Datenvermeidung und Datensparsamkeit

Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese 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. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

Löschung und Speicherbegrenzung

Personenbezogene Daten, 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 ist.

Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten 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.

Vertraulichkeit, Verfügbarkeit und Integrität

Personenbezogene Daten müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene technisch organisatorische Maßnahmen (TOMs) gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

7. Erhebung/Verarbeitung von personenbezogenen Daten

Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen. Hierbei sind auch die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäß Art. 9 Abs. 1 DSGVO 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.
Rechtliche Grundlagen für die Verarbeitung personenbezogener Daten sind u.a.:

- Einwilligung der betroffenen Person.
- Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich.
- Erfüllung einer rechtlichen Verpflichtung.
- Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person.
- Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.
- Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten..

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.

Grundsätzlich ist eine Zweckänderung dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Die Prüfung dieser Tatsache ist zu

einem ordnungsgemäßen Nachweis zu dokumentieren. Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person durch den Verantwortlichen eingeholt wird oder eine sonstige Rechtfertigung vorliegt. 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 des Unternehmens besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der/die DSB zu kontaktieren.

8. Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb der Jäger Group oder an Empfänger innerhalb der Jäger Group unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten. Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden.

Im Falle einer Datenübermittlung an einen Empfänger außerhalb der Jäger Group in einem Drittstaat muss dieser ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt.

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

9. Auftragsverarbeitung

Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten (z. B. Erhebung, Löschung = Entsorgung) bzw. mit Tätigkeiten (z. B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, so ist der DSB vor der Beauftragung unter Vorlage des den Anforderungen des Art. 28 DSGVO genügenden Vertragsentwurfs und der Kriterien der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren.

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

10. 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. Betroffene können Ihre Rechte gegenüber jedem Unternehmen der Jäger Group geltend machen. Entsprechend werden die Unternehmen ein solches Begehren umgehend an die AJH weiterleiten.

Auskunftsrecht

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.
Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.

Recht auf Löschung, Sperrung und Berichtigung

Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.
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.

Widerspruchsrecht

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.
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.

11. Vertraulichkeit der Verarbeitung

Eine unbefugte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten 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.

Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.

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 (TOMs) 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 Datenschutzmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

13. Datengeheimnis

Die Mitarbeiter der Jäger Group werden in durch die Vereinbarung des Arbeitsvertrages zur Einhaltung des Datengeheimnisses verpflichtet. Diese Verpflichtung gilt auch über die Dauer des Beschäftigungsverhältnisses hinaus.

14. Datenschutzkontrolle

Die Einhaltung der Vorgaben, die sich aus dieser Richtlinie 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.

15. Verarbeitungsverzeichnis

Das Datenschutzmanagement führt ein Verarbeitungsverzeichnis nach Art. 30 DSGVO und aktualisiert dieses fortlaufend. Alle neuen Verarbeitungsprozesse werden vor Einführung geprüft, bewertet und, sofern personenbezogene Daten verarbeitet werden, im Verarbeitungsverzeichnis dokumentiert.
Dies gilt sowohl bei Neueinführung von Prozessen als auch bei Änderung bereits bestehender Prozesse und Software.

16. Datenschutzvorfälle

Jeder Mitarbeiter soll unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle) melden.

In Fällen von beispielsweise

- unrechtmäßiger Übermittlung personenbezogener Daten an Dritte,
- unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten, oder
- bei Verlust personenbezogener Daten

sind die im Unternehmen vorgesehenen Meldungen (über den Workflow im Windream BPM Client) unverzüglich vorzunehmen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.

17. Verantwortlichkeiten und Sanktionen

Die Geschäftsleitung ist für die verordnungskonforme Datenverarbeitung personenbezogener Daten verantwortlich.

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

Es ist eine Managementaufgabe der Geschäftsleitung, 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. Bei Datenschutzkontrollen durch Behörden ist der Datenschutzbeauftragte umgehend zu informieren.

Der Datenschutzbeauftragte ist Ansprechpartner für den Datenschutz. Er kann Kontrollen durchführen und hat die Mitarbeiter mit den Inhalten der Datenschutzrichtlinien vertraut zu machen. Die Geschäftsleitung ist verpflichtet, den Datenschutzbeauftragten in seiner Tätigkeit zu unterstützen. Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen der Datenschutzbeauftragten rechtzeitig über neue Verarbeitungen personenbezogener Daten informieren. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Datenschutzbeauftragte schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten.

Die Geschäftsleitung hat sicherzustellen, dass ihre Mitarbeiter im erforderlichen Umfang zum Datenschutz geschult werden. Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht werden in vielen Staaten auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

18. Der Datenschutzbeauftragte

Die AJH hat gemäß Art. 37 DSGVO einen betrieblichen Datenschutzbeauftragten (DSB) konzernweit für alle Unternehmen der Jäger Group bestellt.

Der DSB nimmt die ihm kraft Gesetzes und aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seines Fachwissens sowie seiner beruflichen Qualifikation wahr.
Der Datenschutzbeauftragte unterrichtet und berät die Unternehmensleitung sowie die Arbeitnehmer hinsichtlich ihrer Datenschutzrechte und -pflichten. Ihm obliegt die Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Mitarbeiter. Im Falle risikoreicher Datenverarbeitungen steht der DSB dem Verantwortlichem beratend bei der Abschätzung des Risikos zur Seite.

Der DSB berichtet unmittelbar der Unternehmensleitung.
Der DSB wird frühzeitig in alle Datenschutzfragen eingebunden und wird sowohl von der Unternehmensleitung als auch den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt.

Soweit es sich aufgrund organisatorischer als notwendig erweist, ernennt die Geschäftsleitung im Benehmen mit dem DSB für die jeweilige Organisationseinheit einen Datenschutzkoordinator. Der Koordinator ist also insoweit ein dem DSB fachlich zugewiesener Mitarbeiter zur Einhaltung der für das Unternehmen geltenden Datenschutzvorschriften. Er informiert den DSB über vor Ort aufgetretene Datenschutzfragen. Er erhebt die Angaben über in seinem Zuständigkeitsbereich gesondert eingesetzte Verfahren und gibt die Meldung an den DSB weiter.

Jeder Mitarbeiter kann den DSB mit Fragen und Anliegen zum Datenschutz konsultieren. Der DSB ist in Bezug auf die konsultierende Person zur Vertraulichkeit verpflichtet.

Der DSB erstellt jedes Jahr einen Jahresbericht. Hierin sind insbesondere vorgekommene Datenschutzverstöße und Beschwerden sowie die jährlich durchzuführende Risikobewertung zu dokumentieren.

Datenschutzbeauftragte:

Arnold Jäger Holding GmbH
SRAin Isabel Müller-Wilckens
Telefon 0511-5358-218
E-Mail: dataprotection@jaegergroup.com

19. Inkraftsetzung

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

Änderungen dieses Dokuments liegen in der Verantwortung des Zuständigen für Datenschutzmanagement.

Dieses Dokument ist allen Mitarbeitern zugänglich zu halten.

Marius-Quintus Jäger Sebastian Jäger Dr. Andreas Jäger

25.01.2019