Raiffeisen Hohe Mark Hamaland eG

Datenschutzleitlinie [DSL]

Raiffeisen Hohe Mark Hamaland eG

genoBIT GmbH
Beratung · Information · Technologie

1. Einleitung

Die vorliegende Datenschutzleitlinie [DSL] formuliert den Stellenwert des Datenschutzes für unser Unternehmen. Sie stellt unsere Ziele und Leitsätze in diesem Bereich dar und skizziert den Aufbau des Datenschutzmanagements [DSM], über das wir uns selbst verpflichten, einen angemessenen Schutz personenbezogener Daten/Informationen einzuhalten. Die Wahrung von Persönlichkeitsrechten und die Einhaltung gesetzlicher Bestimmungen zum Datenschutz sind wesentliche Bestandteile unseres Selbstverständnisses. Dies ist unsere Verantwortung - gegenüber unseren Kunden, unseren Mitarbeitern und Geschäftspartnern.

2. Begriffsdefinitionen

Innerhalb dieser Leitlinie werden verschiedene Begriffe verwendet, die zusammenfassend innerhalb der folgenden Abbildung dargestellt werden:

Begriff	Erläuterungen/Beschreibung
Personenbezogene Daten/ Betroffene Person	„Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [im Folgenden „betroffene Person"] beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Onlinekennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
Verarbeitung	Als „Verarbeitung" wird jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter 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, angesehen.
Verantwortlicher	„Verantwortlicher" ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
Datenschutzorganisation	Die Datenschutzorganisation gewährleistet, dass alle relevanten Aufgaben und Regelungen im Bereich des Datenschutzes angemessen wahrgenommen und umgesetzt werden. Kerninhalte sind die Einrichtung von aufbau- und ablauforganisatorischen Regelungen sowie die Definition der erforderlichen Prozesse zum Datenschutz. Dazu gehört ebenfalls eine angemessene Ausgestaltung der personellen Ressourcen.
Datenschutzleitlinie [DSL]	Die Datenschutzleitlinie [DSL] wird durch die Geschäftsführung verabschiedet und ist das „öffentliche Bekenntnis der Geschäftsführung" zum sicheren Umgang mit personenbezogenen Daten. Dieses Dokument ist in Verbindung mit weiteren Strategien des Unternehmens von zentraler Bedeutung und hat allgemein gültigen Charakter.

Begriff	Erläuterungen/Beschreibung
Datenschutzkonzept [DSK]	Das Datenschutzkonzept [DSK] beschreibt die Vorgehensweise zur Planung, Umsetzung, Kontrolle und kontinuierlichen Verbesserung der ergriffenen Datenschutzmaßnahmen innerhalb des Unternehmens.
Datenschutzmanagementsystem [DSMS]	Das Datenschutzmanagementsystem [DSMS] ist ein ganzheitliches Konzept zum sicheren Umgang mit personenbezogenen Daten innerhalb des Unternehmens. Bestandteile eines solchen Systems sind neben den Mitarbeitern das Management, mögliche Ressourcen als auch der eigentliche Prozess, der für den Aufbau und die kontinuierliche Verbesserung des Datenschutzniveaus im Unternehmen verantwortlich ist.
Datenschutzrichtlinie [DSR]/ Arbeitsanweisung zum Datenschutz	Die Datenschutzrichtlinie [DSR] bzw. Arbeitsanweisung zum Datenschutz beschreibt die konkreten Aufgaben, Maßnahmen und Regelungen sowie Zuständigkeiten für die Mitarbeiter im Unternehmen, um die gesetzten Datenschutzziele zu erreichen.
Datenschutzverletzung	Als Datenschutzverletzung wird die Einschränkung oder der Verlust der definierten Schutzziele Verfügbarkeit/Belastbarkeit, Vertraulichkeit oder Integrität von personenbezogenen Daten verstanden. Die Entscheidung darüber, ob es sich um einen meldepflichtigen Vorfall [an die zuständige Aufsichtsbehörde] handelt, wird anhand möglicher Auswirkungen für die betroffene Person zusammen mit dem Datenschutzbeauftragten ermittelt.

Abb. 1: Übersicht Begriffsdefinitionen

3. Geltungsbereich

Datenschutz ist ein ganzheitlicher Ansatz, der sowohl personelle, infrastrukturelle, organisatorische und technische Aspekte umfasst. Der Geltungsbereich für den Datenschutz umfasst alle Bereiche unseres Unternehmens, in denen personenbezogene Daten verarbeitet werden. Daran angeknüpft sind externe Prozesse, Unternehmensbereiche und Auslagerungen. Unsere internen Anforderungen übertragen wir somit grundsätzlich auch auf unsere externen Partner oder Dienstleister.

4. Ziele des Datenschutzes

Unser vorrangiges Ziel ist die Wahrung der Persönlichkeitsrechte der betroffenen Person und die Einhaltung gesetzlicher Bestimmungen zum Datenschutz. Als zentrale Anforderungen zum Schutz und zur Sicherheit personenbezogener Daten und Informationen klassifizieren wir diese entsprechend den gesetzlichen Vorgaben nach folgenden Schutzzielen:

Schutzziel	Beschreibung und Hinweise
Verfügbarkeit [Belastbarkeit]	Die Verfügbarkeit von personenbezogenen Daten ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können. Die Belastbarkeit ist vorhanden sofern eine angemessene Widerstandsfähigkeit/Resilienz personenbezogener Daten gegen eine mögliche Beschädigung oder Zerstörung besteht.
Vertraulichkeit	Vertraulichkeit ist der Schutz vor unbefugter Preisgabe personenbezogener Daten. Sie dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Schutzziel	Beschreibung und Hinweise
Integrität	Integrität bezeichnet die Sicherstellung der Korrektheit [Unversehrtheit] von personenbezogenen Daten [vollständig und unverändert].

Abb. 2: Ziele des Datenschutzes

Diese Ziele gelten für alle personenbezogenen Daten im Unternehmen, unabhängig vom verwendeten Medium oder der Verarbeitungsart, manuell oder automatisiert. Sie unterliegen unserer Verantwortung.

5. Abgrenzung der Schutzziele zur Informationssicherheit

Das Informationssicherheitsmanagement betrachtet grundsätzlich alle sensiblen Daten und Informationen in einem Unternehmen, unabhängig vom verwendeten Medium [papierhaft, elektronisch oder in sonstiger Form]. Darin inbegriffen natürlich auch personenbezogene Daten als Teilmenge. Durch eine enge Verknüpfung des Informationssicherheitsmanagements mit dem Datenschutzmanagement ergeben sich viele Synergieeffekte. Zu beachten bleibt jedoch, dass die verfolgten Ziele nicht in allen Bereichen identisch sind. Im Folgenden wird die Abgrenzung zwischen der Informationssicherheit und dem Datenschutz verdeutlicht.

	Informationssicherheit	Datenschutz
Schutzzweck	Dient primär dem Interesse des Unternehmens.	Dient dem Interesse der betroffenen Person [und der Gesellschaft].
Anspruchsgrundlage	Grundsätzlich keine gesetzliche Anforderung zur Umsetzung, ausgenommen Spezialgesetze, Sondernormen oder sonstige regulatorische Anforderungen.	Gesetzliche Anforderung durch die EU-Datenschutz-Grundverordnung [EU-DSGVO].
Anwendungsbereich	Bezieht sich auf alle sensiblen Daten und Informationen des Unternehmens, unabhängig vom verwendeten Medium.	Bezieht sich ausschließlich auf alle Verarbeitungstätigkeiten in Verbindung mit personenbezogenen Daten.
Funktion	Schutz der Vermögenswerte [Daten und Informationen] eines Unternehmens vor Beeinträchtigung oder Verlust der Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität.	Schutz von personenbezogenen Daten der betroffenen Person vor Beeinträchtigung oder Verlust der Schutzziele Verfügbarkeit [Belastbarkeit], Vertraulichkeit und Integrität.
Maßnahmen	Umsetzung von technischen und organisatorischen Maßnahmen zum Schutz der Vermögenswerte und somit auch Teile des Datenschutzes.	Umsetzung von technischen und organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten und somit auch Teile der Informationssicherheit.

Abb. 3: Abgrenzung zur Informationssicherheit

6. Leitsätze für den Datenschutz

Für den Datenschutz in unserem Unternehmen gelten folgende Leitsätze:

Leitsätze zum Datenschutz
▪ **Leitsatz 1:**

Bei der Gestaltung und Erreichung der Geschäftsziele bedarf es der stetigen Intension, den Schutz der Persönlichkeitsrechte unserer Kunden, Mitarbeiter und Geschäftspartner angemessen zu berücksichtigen.

- **Leitsatz 2:**
  Datenschutz ist ein Qualitätsmerkmal, das sich positiv auf das Vertrauen im Unternehmen selbst aber auch gegenüber dem Kunden und somit auf die Kundenbeziehung auswirkt.
- **Leitsatz 3:**
  Jeder trägt Verantwortung im Umgang mit seinen eigenen personenbezogenen Daten aber auch mit denen unserer Kunden, Mitarbeiter und Geschäftspartner.
- **Leitsatz 4:**
  Wir gehen mit fremden personenbezogenen Daten so um, wie wir es selbst ebenfalls erwarten würden - sensibel und gesetzeskonform.

Abb. 4: Leitsätze zum Datenschutz

Die Leitsätze zum Datenschutz sind für alle unsere Mitarbeiter verbindlich. Aus ihnen ergeben sich konkrete Handlungsanweisungen, die als eigenständige Dokumente und Regelungen niedergeschrieben sind.

7. Datenschutzmanagement [DSM]

Aufgrund der Verantwortung und des hohen Stellenwerts des Datenschutzes für unserer Unternehmen, wurde von der Geschäftsführung als Verantwortlicher ein Datenschutzmanagementsystem [DSMS] etabliert. Die eingerichtete Datenschutzorganisation übernimmt die operativen Aufgaben des Datenschutzmanagementprozesses und unterstützt damit die Geschäftsführung bei der Umsetzung, Einhaltung und Überprüfung der datenschutzrechtlichen Anforderungen.

7.1 Aufbau der Datenschutzorganisation

Als zentrale Funktion für den Datenschutz wurde Herr Hubert Lütke Laxen schriftlich zum Datenschutzbeauftragten [DSB] des Unternehmens benannt. Er wird in seiner Tätigkeit durch Herrn Lukas Lensing in der Funktion als Verbindungsstelle zum Datenschutz unterstützt.

Jegliche Anfragen zum Datenschutz werden über die Verbindungsstelle kanalisiert. Der Datenschutzbeauftragte ist in alle Sachverhalte und Prozesse zum Datenschutz angemessen einzubinden. Seine primäre Aufgabe liegt darin, Datenschutz im Unternehmen anzuleiten und die Umsetzung, Aufrechterhaltung und kontinuierliche Weiterentwicklung zu fördern sowie die Einhaltung zu kontrollieren.

Er berichtet in seiner Funktion direkt an die Geschäftsführung. Sowohl er als auch die Verbindungsstelle zum Datenschutz werden durch die Mitarbeiter des Unternehmens ausreichend in ihrer Arbeit unterstützt. Sofern notwendig, werden weitere Funktionsbereiche projektbegleitend und prozessunabhängig eingebunden. Weitere Aufgaben des Datenschutzbeauftragten ergeben sich aus der Anlage 1.

7.2 Das Datenschutzkonzept [DSK]

Das Datenschutzkonzept [DSK] beschreibt die Vorgehensweise zur Planung, Umsetzung, Kontrolle und kontinuierlichen Verbesserung des Datenschutzes bzw. der ergriffenen Datenschutzmaßnahmen innerhalb des Unternehmens. Dies ist keine einmalige Tätigkeit, sondern vielmehr ein Prozess, der dafür sorgt, das Datenschutzniveau im Unternehmen aufrechtzuerhalten und kontinuierlich zu verbessern. Der Fokus liegt dabei immer auf dem Schutz der personenbezogenen Daten im Rahmen der Verarbeitung.

8. Verpflichtung und Verantwortung der Geschäftsführung

Die Geschäftsführung trägt die Gesamtverantwortung für die im Unternehmen verarbeiteten personenbezogenen Daten, auch gegenüber den Kunden, Mitarbeitern und Geschäftspartnern. Ihr kommt zudem eine besondere Vorbildfunktion zu. Sie unterstützt und begleitet das Datenschutzmanagement [DSM] und sorgt dafür, dass die definierten Maßnahmen umgesetzt und eingehalten werden. Sie stellt der Datenschutzorganisation entsprechende sachliche, finanzielle und personelle Ressourcen zur Verfügung, die eine Umsetzung, Einhaltung und Weiterentwicklung des Datenschutzes im Unternehmen gewährleisten.

9. Verpflichtung und Verantwortung der Mitarbeiter

Allen Mitarbeitern ist die Bedeutung der Wahrung von Persönlichkeitsrechten und die Einhaltung gesetzlicher Bestimmungen zum Datenschutz bewusst.

Jeder trägt die Verantwortung für den korrekten und sicheren Umgang mit personenbezogenen Daten. Sie sind verpflichtet, die Regelungen und Vorgaben einzuhalten bzw. bei der täglichen Arbeit zu berücksichtigen. Dabei handeln sie eigenverantwortlich im Sinne der gesetzlichen Grundlage als auch den internen Regelungen und Richtlinien und leisten dadurch ihren wichtigen und aktiven Beitrag zum Schutz der personenbezogenen Daten im Unternehmen.

Die Nichteinhaltung sowie der fahrlässige Umgang mit personenbezogenen Daten, entgegen den getroffenen Regelungen und Gesetzen, können zu arbeitsrechtlichen Konsequenzen führen und/oder zu einer Haftung des Unternehmens bzw. einer persönlichen Haftung des Arbeitnehmers.

10. Weiterentwicklung und kontinuierliche Verbesserung

Die Überprüfung des angemessenen Schutzes personenbezogener Daten erfolgt regelmäßig im Rahmen von Kontrollhandlungen im Datenschutzmanagement. Das Ergebnis gibt Aufschluss über mögliche Anpassungsbedarfe.

Darüber hinaus erfolgt eine anlassbezogene oder mindestens jährliche Aktualisierung aller Regelungen mit Datenschutzbezug des Unternehmens sowie weiterer Konzepte. Erkannte Datenschutzverletzungen werden grundsätzlich ausgewertet bzw. analysiert, um ein wiederholtes Eintreten zu verhindern. Regelmäßige Schulungen und Sensibilisierungen der Mitarbeiter sorgen ebenfalls für eine Erhöhung des Schutzes personenbezogener Daten im Unternehmen.

Diese und weitere Maßnahmen sorgen für eine stetige Weiterentwicklung und kontinuierliche Verbesserung des Datenschutzes.

11. Verabschiedung der Datenschutzleitlinie und Art der Bekanntgabe

Unsere Datenschutzleitlinie wurde von der Geschäftsführung verabschiedet und veröffentlicht. Änderungen und Ergänzungen bedürfen der Schriftform und müssen von der Geschäftsführung verabschiedet werden.

12. Weiterführende Informationen und Unterlagen:

1. IT-Strategie des Unternehmens
2. Datenschutzkonzept [DSK]
3. Datenschutzrichtlinie [DSR]
4. Konzept zur Löschung personenbezogener Daten