Raiffeisen Landesbank Vorarlberg

Datenschutz-Organisationsrichtlinie

der Raiffeisen Landesbank Vorarlberg mit Revisionsverband eGen für den Umgang mit personenbezogenen Daten

INHALTSVERZEICHNIS

1. GELTUNGSBEREICH

Die Richtlinie ist für alle Mitarbeiter:innen der RLB, die im Zuge ihrer Tätigkeiten personenbezogene Daten verarbeiten, anzuwenden.

Aus Gründen der besseren Lesbarkeit wird in diesem Dokument auf die geschlechtsspezifische Doppelnennung verzichtet.

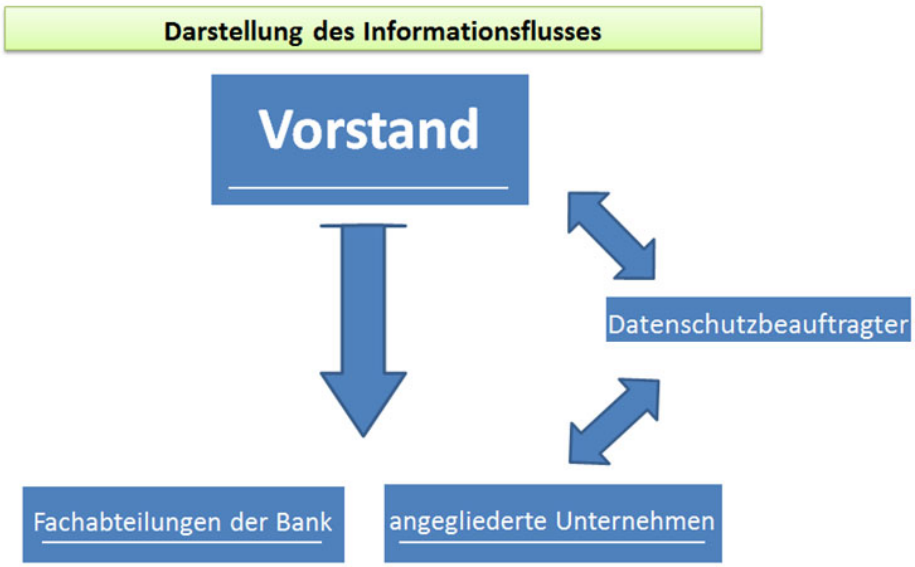
2. BESCHREIBUNG DES STELLENWERTES UND DER ALLGEMEINEN ZIELSETZUNG

Sicherheit ist ein wesentlicher Bestandteil unseres Markenversprechens. Dies bedeutet, dass die Raiffeisen Landesbank Vorarlberg (nachfolgend kurz „RLB") dem Schutz der personenbezogenen Daten hohe Aufmerksamkeit widmet. Die entsprechenden Vorgaben werden in unserer Datenschutzstrategie beschrieben.

3. DATENSCHUTZ-ORGANISATION DER RLB

In dieser Richtlinie werden die Struktur der Datenschutzorganisation im Geschäftsbereich der RLB, sowie die Aufgaben der Datenschutzorganisation im Detail erläutert. Zudem wird der einzuhaltende Informationsprozess („Data Breach Notification Prozess") im Falle einer Datenschutzverletzung beschrieben. Wie die Datenschutzstrategie gilt diese Richtlinie für die Geschäftsleitung sowie alle Arbeitnehmer:innen der RLB.

4. DATENSCHUTZBEAUFTRAGTE:R IM INFORMATIONSFLUSS ZWISCHEN VORSTAND UND OPERATIVEN EINHEITEN



Die Verantwortung für die Einhaltung der gesetzlichen und internen Datenschutzvorschriften liegt beim Vorstand der RLB bzw. dem:der §9 VStG Verantwortlichen. Die Datenschutz-Organisation unterstützt das Management in der Wahrnehmung seiner Verantwortung und stellt die hierfür erforderlichen Prozesse zur Verfügung. Ansprechpartner:in im Zusammenhang mit Datensicherheit sind der:die Datenschutzbeauftragte, der CISO sowie die Sicherheits-Beauftragten.

Das Management ist verpflichtet, den:die Datenschutzbeauftragte:n in seiner:ihrer Tätigkeit zu unterstützen, ihm:ihr entsprechende Ressourcen, Berechtigungen und Zugänge zu Datenverarbeitungsanlagen zur Verfügung zu stellen. Der:die Datenschutzbeauftragte ist Geheimnisträger:in gemäß §5 „Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten"[1], zudem steht ihm:ihr in bestimmten Fällen das gesetzliche Aussageverweigerungsrecht zu. Die Fachabteilungen informieren den:die Datenschutzbeauftragte:n über die Einführung sowie Änderung von kritischen EDV-Systemen in deren Einflussbereich, bei welchen ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zu erwarten ist sowie bei Verarbeitung sensibler Daten (Art 9 und 10 der „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG"[2]).
Die Aufgabe des:der Datenschutzbeauftragten ist die Beratung in allen datenschutzrechtlichen Belangen und Überprüfung der Einhaltung der Datenschutzgrundverordnung. Er:sie informiert den Vorstand unmittelbar, dieser trifft die notwendigen Entscheidungen.

5. DATENSCHUTZMANAGEMENT

Aus der DSGVO ergibt sich die Verpflichtung für die RLB eine:n Datenschutzbeauftragte:n zu bestellen. Der:die Datenschutzbeauftragte ist an Verschwiegenheitspflichten gebunden und zur Geheimhaltung verpflichtet (§5 DSG, Art. 38 Abs 5 DSGVO, §38 Bankwesengesetz).

5.1 Aufgaben der Datenschutzbeauftragten

Die Rechtsgrundlagen für den:die Datenschutzbeauftragte:n sind in den Artikeln 37 bis 39 beschrieben.

Die Aufgaben des internen Datenschutzbeauftragten umfassen insbesondere:

- Mitarbeit und Teilnahme an den Sitzungen des Raiffeisensektors;
- Schulungen für Arbeitnehmer:innen, welche mit personenbezogenen Daten arbeiten, definieren
- Überwachung der Einhaltung der nationalen und internen datenschutzrechtlichen Vorgaben
- Information über mögliche Datenschutzrisiken (z.B.: Gesetzesänderungen, aktuelle Gerichtsurteile, Bedrohungsszenarien) an den Vorstand sowie den Sektor
- Regelmäßige Berichterstattung an den Vorstand
- Abstimmung im Sektor zur Gewährleistung der einheitlichen Umsetzung der internen Datenschutzvorgaben

[1] nachfolgend kurz „DSG"
[2] nachfolgend kurz „DSGVO"

- Beratung bei speziellen Verarbeitungs-Konstellationen, wie beispielsweise Profiling, Big-Data Auswertungen und besonderer Kategorien personenbezogener Daten nach Art. 9 und 10 DSGVO
- Mitwirkung bei der Führung eines Verzeichnisses von Verarbeitungstätigkeiten
- Unterstützung der Durchführung einer Risikobewertung (aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können) sowie, falls erforderlich, Mitwirkung bei der Durchführung einer Datenschutz-Folgenabschätzung vor Einführung einer Datenverarbeitung in Abstimmung mit dem für den jeweiligen Fachbereich Zuständigen des Verantwortlichen.

5.2 Die Datenschutzkontaktperson

Zur Durchführung der Aufgaben von der Geschäftsleitung wird eine Datenschutzkontaktperson ernannt. Die Datenschutzkontaktperson ist vor Ort der:die erste Ansprechpartner:in für alle datenschutzrechtlichen Fragestellungen. Ihr obliegt unter anderem:

- Schulung der Arbeitnehmer:innen, die mit personenbezogenen Daten
- arbeiten;
- Überwachung der Einhaltung der internen datenschutzrechtlichen Vorgaben;
- Unterstützung der Durchführung einer Risikobewertung (aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können) sowie, falls erforderlich, Mitwirkung bei der Durchführung einer Datenschutz-Folgenabschätzung vor Einführung einer Datenverarbeitung in Abstimmung mit dem:der für den jeweiligen Fachbereich Zuständigen des:der Verantwortlichen.
- Erstellung und Führung eines Verzeichnisses von Verarbeitungstätigkeiten. Die Erstellung erfolgt unter Anleitung des:der Datenschutzbeauftragten.
- Meldungen über Verletzungen des Schutzes personenbezogener Daten (z.B.: Datenverlust) an den:die Datenschutzbeauftragte:n;
- Regelmäßige Berichterstattung an den:die Datenschutzbeauftragte:n;
- Abstimmung mit dem:der Datenschutzbeauftragten zur Gewährleistung der einheitlichen Umsetzung der internen Datenschutzvorgaben;
- Einbindung des:der Datenschutzbeauftragten bei Datenverarbeitungsvorhaben

6. ABSTIMMUNGEN IM SEKTOR

Die Datenschutzbeauftragten der „RBGÖ" bilden bundesweite Arbeitsgruppen. Ihre Aufgabe ist die Abstimmung und Beratung der Vorgehensweise und die Festlegung gemeinsamer Maßnahmen. Ebenso dient diese Zusammenarbeit als Forum für einen regelmäßigen Erfahrungsaustausch. Somit kann ein gemeinsamer und einheitlicher Datenschutzstandard in der „RBGÖ" gewährleistet werden. Die Entscheidungskompetenzen der Unternehmensleitung als Organ des Unternehmens bleiben von dieser Zusammenarbeit unberührt.

7. EINBETTUNG DES DATENSCHUTZES IN DIE ABLAUFORGANISATION

Die Datenschutzbeauftragten sind verpflichtet und berechtigt, regelmäßig und nach risikoorientierten Gesichtspunkten die Datenverarbeitungen in Abstimmung mit der Revision zu überprüfen. Die Datenschutzbeauftragten berichten direkt an den Vorstand. Die Inhalte der

Datenschutzrichtlinien sind den Arbeitnehmern:innen nachweislich bekannt zu machen. Bei dieser Tätigkeit wirken die Datenschutzkontaktpersonen federführend.
Der jährliche Statusbericht des:der Datenschutzbeauftragten über die durchgeführten Tätigkeiten und ggf. die datenschutzrelevanten Vorfälle in der einzelnen Gesellschaft werden dem Vorstand vorgelegt.

8. RISIKOORIENTIERTE AUSWAHL DER SCHUTZMAßNAHMEN

Nach den Vorgaben aus Art. 25 DSGVO „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" werden Schutzmaßnahmen entsprechend dem Risiko, nach dem Stand der Technik sowie unter Erwägung wirtschaftlicher Kriterien eingesetzt. An dieser Stelle sei auf die „Checkliste zur Beachtung der Anforderungen an Privacy-by Design / Privacy-by-Default"[3] verwiesen.

9. VERTRETUNGSREGELUNG FÜR DIE DSKP

Die Datenschutzkontaktperson hat dafür Sorge zu tragen, dass im Falle einer Abwesenheit Meldepflichten gewahrt werden und der Informationsaustausch gewährleistet wird. Die Bewertung von notwendigen, vorzunehmenden Maßnahmen wird stets durch den Vorstand veranlasst und durch den:die Datenschutzbeauftragte:n begleitet.

10. MELDUNGEN VON VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN

10.1 Data Breach

Verletzungen des Schutzes personenbezogener Daten sind unrechtmäßige oder unbeabsichtigte Datenvernichtungen, -verluste, -veränderungen, -offenlegungen oder sonstige Datenverarbeitungen (nachfolgend kurz „Datenschutzverletzung")[4]. Es ist unerheblich, ob die Datenschutzverletzung mit Vorsatz, unbewusst, fahrlässig oder durch (technische) Fehler während der Datenverarbeitung erfolgt ist. Unwesentlich ist auch, welche Art von Datenträger betroffen ist oder welche Art der Verarbeitung zur Verletzung geführt hat.

Beispiele für Datenverletzungen sind[5]

- Datenvernichtung: wenn Daten nicht mehr existieren oder nicht mehr in einer Form existieren, die eine Verarbeitung ermöglicht (**Verfügbarkeitsverletzung**)

[3] eine interne Datenschutz-Richtlinie zum Art. 25 DSGVO
[4] Art. 4 Z 12 DSGVO: (Die) „Verletzung des Schutzes personenbezogener Daten" (ist) eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden
[5] WP250 der Art. 29 Gruppe, Guidelines on Personal data breach notification under Regulation 2016/679, Seite 5 ff.

- Schädigung von personenbezogenen Daten: insbesondere Veränderung, Beschädigung, Unvollständigkeit sowie auch die Genauigkeit von Daten (**Integritätsverletzung**)
- Datenverlust: wenn personenbezogene Daten existieren, jedoch keine Kontrolle oder Zugriffsmöglichkeit mehr besteht (ebenfalls eine **Verfügbarkeitsverletzung**)
- Unbefugte Offenlegung beziehungsweise unbefugter Zugang: wenn Empfänger:in unbefugt Daten erhalten oder unbefugt Zugang zu Daten erlangen (**Vertraulichkeitsverletzung**)

Um der Rechenschaftspflicht nachzukommen, werden folgende Detail-Regelungen durch den Vorstand getroffen:

1. Erweiterung des bestehenden Sicherheits-Organigramms um ein Datenschutz-Sicherheitsvorfallteam
2. Abstimmung mit weiteren bestehenden Verpflichtungen zum Melden von Sicherheitsvorfällen (z.B. NIS-Gesetz, ZaDiG).
3. Konkretisierung der Meldepflichten in einer Dienstanweisung für alle Arbeitnehmer:innen und Führungskräfte: verpflichtende Erfassung in der Datenbank „DSGVO Datenschutzverletzungen" sowie das Erstellen eines RSP-Ticket an den Datenschutzbeauftragten
4. Berücksichtigen von Outsourcing: Auftragsverarbeiter:innen müssen risikobasiert Datenschutzvorkehrungen treffen sowie Unterstützung bieten und ebenfalls Meldepflichten einhalten. Die Datenschutzkonaktperson bestimmt routinemäßige Überprüfung der Auftragsverarbeite:innen, die durch Arbeitnehmer:innen oder durch den:die Datenschutzbeauftragte:n vorzunehmen sind
5. Zur Erfüllung der Melde- und Informationspflicht bei Datenschutzverletzungen wird ein RBGV einheitliches Meldeformular benutzt welches Art. 33 Abs 3 DSGVO entspricht.
6. vorbeugende Maßnahmen zur Risikominimierung werden durch die DSKp sowie den:die Datenschutzbeauftragte:n dokumentiert, um die Rechte und Grundfreiheiten der Betroffenen zu wahren.
7. Einrichtung eines Registers nach Art. 33 Abs 5 DSGVO (Datenbank „DSGVO Datenschutzverletzungen"), in dem alle Verletzungen des Schutzes personenbezogener Daten dokumentiert werden, einschließlich aller im Zusammenhang mit der Verletzung stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen[6]. Sollte auch keine Meldung an die Datenschutzbehörde oder an Betroffene erfolgen oder eine Datenschutzverletzung auch nur vermutet werden, ist ein begründeter Eintrag in der Datenbank vorzunehmen und zu kategorisieren. Hierzu ergeht eine Dienstanweisung an alle Arbeitnehmer:innen, die eine verpflichtende Meldung vorsieht.

10.2 Melde- und Informationspflicht bei Datenschutzverletzungen

Eine Informationspflicht durch den Vorstand besteht jedenfalls, wenn aufgrund der Datenschutzverletzung voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht.
Dies ist beispielsweise der Fall, wenn dem:der Betroffenen ein physischer, materieller oder immaterieller Schaden entsteht, wie etwa Verlust der Kontrolle über seine personenbezogenen Daten, Identitätsdiebstahl oder -betrug, finanzielle Verluste, Rufschädigung, Verlust der

[6] Art. 33 Abs. 5 DSGVO

Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile.

10.3 Prozess Datenschutzvorfall

Im Falle einer Datenschutzverletzung oder bei Verdacht auf Vorliegen einer Datenschutzverletzung sind Arbeitnehmer:innen sowie Führungskräfte verpflichtet, unverzüglich eine Meldung entsprechend dem dafür eigens festgelegten Prozedere erstatten.

Inwieweit **zusätzlich** eine Meldung an die lokale Aufsichtsbehörde (spätestens innerhalb von 72 Stunden ab Kenntnis der Datenschutzverletzung), an den:die Betroffene:n (Frist unverzüglich nach Kenntnis der Datenschutzverletzung und bei Gefahr für den:die Betroffene:n) oder an die Öffentlichkeit zu erfolgen hat, ist von dem:der Datenschutzbeauftragten in Abstimmung mit dem CISO und dem Vorstand zu prüfen.

Der:die Datenschutzbeauftragte wird nach Erhalt des RSP-Ticket unverzüglich das jeweilige Management über eine derartige Veröffentlichungs-/Meldepflicht informieren. Die weitere Kommunikation nach außen hat durch den:die Sprecher:in des Vorstandes oder durch die:die Handlungsbefugte:n laut Notfallorganisation zu erfolgen. Die involvierten Parteien, abgesehen vom Vorstand, haben ein absolutes **Kommunikationsverbot** nach außen einzuhalten. Das Krisenmanagement erfolgt entsprechend der Beschreibung im aktuellen Krisenhandbuch der RLB & Raiffeisen Österreich.

11. WEITERFÜHRENDE INFORMATIONEN

Folgende Detailbeschreibungen sind im Zusammenhang mit dieser Richtlinie relevant:

- OHB „Datenschutzstrategie - Leitlinie zum Umgang mit personenbezogenen Daten"
- IMS Anleitung „Datenschutzverletzung"
- Dienstanweisung „Datenschutzverletzung"