ESG Governance
Data Privacy

Version 01 / Stand 09.01.2026

ESG Rating-Maßnahme: Data Privacy

- **Awareness-Kommunikation**
  Datenschutzthemen werden laufend über interne Kommunikationskanäle wie das Intranet und Informationsmails kommuniziert.
- **Meldeprozess**
  Ein klar definierter Meldeprozess für Datenschutzvorfälle ist implementiert. Mitarbeitende sind angehalten, mögliche Vorfälle umgehend intern zu melden, um eine schnelle Bewertung und falls erforderlich, wird eine Meldung innerhalb 72 Stunden an die Datenschutzbehörde sichergestellt. Es wird schnellstmöglich der Sachverhalt geklärt (was, wann passiert ist), welche personenbezogenen Daten betroffenen sind und eine Risikoanalyse durchgeführt.
- **Gültigkeit für alle Geschäftsbereiche und Beteiligungen**

Die Datenschutzvorgaben und -maßnahmen gelten übergreifend, also für alle Geschäftsbereiche und die servicierten Beteiligungen. Dadurch wird ein einheitliches Datenschutzniveau gewährleistet und eine konsistente Umsetzung der DSGVO sichergestellt.

- **Klärung der Erhebungszwecke**

Die Zwecke der Erhebung und Verarbeitung personenbezogener Daten sind eindeutig definiert und dokumentiert. Eine Verarbeitung erfolgt ausschließlich zu legitimen, vorher festgelegten Zwecken, die transparent in der öffentlich zugänglichen Erklärung in Bezug auf Art 13 & 14 der DSGVO werden die Erhebungszwecke geklärt.

- **Klärung der Mittel der Datenerhebung**

Die Erhebung personenbezogener Daten erfolgt ausschließlich mit datenschutzkonformen Mitteln und Systemen. Dabei werden technische und organisatorische Maßnahmen eingesetzt, die den Grundsätzen der Datenminimierung, Zweckbindung und Sicherheit entsprechen.

- **Zugriff Dritter und Rechte betroffener Personen**

Dritte erhalten ausschließlich dann Zugriff auf personenbezogene Daten auf Basis vorliegender Rechtmäßigkeit und unter Einhaltung der Datenschutzgrundsätze der Verarbeitung. In solchen Fällen bestehen Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO. Betroffene Personen werden über ihre Rechte umfassend informiert und können diese jederzeit wahrnehmen.

- **Weitergabe personenbezogener Daten an Dritte**

Eine Weitergabe personenbezogener Daten an Dritte erfolgt ausschließlich auf Basis vorliegender Rechtmäßigkeit und unter Einhaltung der Datenschutzgrundsätze der Verarbeitung.

- **Datenschutzmanagementsystem (DSMS) und Audits**

Ein umfassendes Datenschutzmanagementsystem (DSMS) ist implementiert und bildet die Grundlage für die systematische Steuerung, Überwachung (Audit) und Verbesserung des Datenschutzes im Unternehmen. Das DSMS wird regelmäßig überprüft und aktualisiert.

- **Analysen, Risikoabschätzungen und Kontrollen**
  Regelmäßige Datenschutzanalysen sowie interne Kontrollen werden

durchgeführt, um die Wirksamkeit der bestehenden Datenschutzmaßnahmen zu evaluieren. Externe Kontrollen erfolgen im Rahmen der jährlichen Datenschutzprüfungen und setzen jeweils einen wechselnden Schwerpunkt auf ein aktuelles, relevantes Thema. Ergänzt werden diese Maßnahmen durch Risikobewertungen von Verarbeitungstätigkeiten (vergleichbar mit Privacy Impact Assessments) und Datenschutz-Folgenabschätzungen, um die Einhaltung der Datenschutzanforderungen umfassend sicherzustellen.

- **Verantwortlichkeiten auf Vorstandsebene**

Die Verantwortung für die Verarbeitung der Daten sowie die getroffenen Maßnahmen liegt beim Vorstand bzw. Geschäftsleitung. Der Datenschutzbeauftragte berichtet regelmäßig an das Management.

- **Berichte ans Management:** Das Management wird regelmäßig über datenschutzrelevante Themen informiert. Dazu gehören Berichte über potenzielle Risiken, umgesetzte Maßnahmen sowie eventuelle Vorfälle. Zudem erfolgt ein Direct Report des Datenschutzbeauftragten an das Management.
- **Einführung von Kontrollen**

Es besteh ein internes Kontrollsystem zur Überprüfung der Einhaltung datenschutzrechtlicher Anforderungen. Diese Kontrollen werden regelmäßig durchgeführt, dokumentiert und bei Bedarf angepasst, um neue rechtliche oder technische Entwicklungen zu berücksichtigen. Dadurch wird ein fortlaufender Verbesserungsprozess gewährleistet.

- **Löschung personenbezogener Daten**

Anforderungen zur Löschung personenbezogener Daten sind vollständig erfüllt. Es existieren klare und dokumentierte Löschkonzepte, die die gesetzlichen Aufbewahrungsfristen berücksichtigen. Nach Ablauf dieser Fristen werden personenbezogene Daten gelöscht. Diese Prozesse sind technisch und organisatorisch abgesichert und werden regelmäßig überprüft. Damit ist der Löschvorgang eindeutig geregelt und jederzeit nachvollziehbar.

- **Zugang zu personenbezogenen Daten & Richtigstellung**
  Betroffene Personen haben jederzeit die Möglichkeit, Auskunft über die zu ihrer Person gespeicherten Daten zu erhalten. Die entsprechenden Verfahren sind in der Datenschutzerklärung klar beschrieben und intern fest verankert. Auch das Recht auf Berichtigung ist vollständig umgesetzt: Personen können unrichtige oder unvollständige Daten jederzeit korrigieren lassen. Dafür stehen definierte interne Prozesse sowie Kontaktmöglichkeiten zur Verfügung.
  Damit sind sowohl das Auskunftsrecht als auch das Recht auf Richtigstellung umfassend abgedeckt.
- **Verschlüsselung und De-Identifikation**
  Die Sicherheit personenbezogener Daten ist durch umfassende technische und organisatorische Maßnahmen gewährleistet. Alle relevanten Datenübertragungen erfolgen ausschließlich verschlüsselt, sowohl bei der Übermittlung als auch bei der Speicherung. Zusätzlich werden personenbezogene Daten, sofern möglich und zweckmäßig, pseudonymisiert

oder anonymisiert, um das Risiko für betroffene Personen weiter zu minimieren. Diese Maßnahmen entsprechen den Anforderungen von Art. 32 DSGVO und sind im Datenschutzmanagementsystem dokumentiert und implementiert. Damit sind sowohl Verschlüsselung als auch De-Identifikation klar berücksichtigt.

- **Consent Policy / Nutzung personenbezogener Daten für sekundäre Zwecke**
  Personenbezogene Daten werden nicht an Dritte weitergegeben, außer es liegen vertragliche oder gesetzliche Gründe vor. Personenbezogene Daten werden nicht für andere, weitergehende oder kommerzielle Zwecke genutzt oder weitergegeben, etwa für Marketing, Analysen, Verkauf oder Vermietung.
- **Datenschutzprogramme für Lieferanten und Geschäftspartner**
  Das Unternehmen stellt sicher, dass Datenschutzanforderungen auch bei Lieferanten und Geschäftspartnern eingehalten werden. Regelmäßige Prüfungen und Inspektionen werden durchgeführt.
- **Schulungen der Mitarbeitenden**
  Alle Mitarbeitenden erhalten regelmäßig verpflichtende Datenschutzschulungen. Diese stellen sicher, dass datenschutzrechtliche Anforderungen bekannt sind, verstanden werden und im Arbeitsalltag konsequent umgesetzt werden. Dazu bestehen unterschiedliche Auswahlmöglichkeiten; Schulungen vor Ort, online oder selbständig in Form eines WBTs.

Raiffeisenlandesbank Niederösterreich-Wien

Abteilung Outsourcing, Vertragsmanagement und Datenschutz (OVD)
Raiffeisenlandesbank Niederösterreich-Wien
Friedrich-Wilhelm-Raiffeisenplatz 1
1020 Wien
Tel.: +43 05 1700 - 91680
E-Mail: datenschutz@raiffeisenbank.at
http://www.raiffeisenbank.at

Raiffeisenlandesbank
Niederösterreich-Wien