Raiffeisen Landesbank Vorarlberg

Geheimhaltungspflichten

Dienstanweisung zum Bankgeheimnis, Datenschutz und Geschäftsgeheimnissen

INHALTSVERZEICHNIS

1. GELTUNGSBEREICH

Diese Dienstanweisung gilt für Mitarbeiter:innen der Vorarlberger Raiffeisenbanken, der Raiffeisen Landesbank Vorarlberg samt Töchterunternehmen wie der Raiffeisen-Immobilien GmbH, der RVM Raiffeisen Versicherungsmakler Vorarlberg GmbH und der Raiffeisen Direkt Service Vorarlberg GmbH (im Folgenden Dienstgeber:innen genannt).

Die Vorgaben betreffend das Bankgeheimnis gelten nur für Bankmitarbeiter:innen und Dienstleister:innen die für die Bank tätig sind, beziehungsweise waren.

2. ZIELSETZUNG

Diese Dienstanweisung dient zur Umsetzung gesetzlicher Vorgaben.

Eine Meldung von Datenschutzverletzungen bringt für den:die Mitarbeiter:in keine zusätzlichen Sanktionen mit sich, sie wirkt sogar entlastend.

3. KURZZUSAMMENFASSUNG

Arbeitnehmer:innen sind zu vertragsgemäßer, gewissenhafter Arbeit und berufsüblicher Sorgfalt unter Beachtung der Anweisungen des Arbeitgebers verpflichtet. Bei einer Dienstanweisung handelt es sich um einen verbindlichen Arbeitsauftrag an einzelne Personen oder Personengruppen. Die Dienstanweisung beschreibt, wie sich jemand konkret zu verhalten oder ein Vorgang abzulaufen hat (Muss-Bestimmungen).

Im Falle eines Verstoßes gegen diese Dienstanweisung haben Mitarbeiter:innen unter Umständen arbeitsrechtliche als auch strafrechtliche Folgen zu tragen sowie Schadenersatz zu leisten.

4. ANSPRECHPARTNER:IN

5. GEHEIMNISPFLICHTEN

5.1 Bankgeheimnis

5.2 geheimhaltungspflichtiger Personenkreis

"Kreditinstitute, ihre Gesellschafter:innen, Organmitglieder, Beschäftigte sowie sonst für die Kreditinstitute tätige Personen dürfen Geheimnisse, die ihnen ausschließlich aufgrund der Geschäftsverbindungen mit Kund:innen oder aufgrund des § 75 Abs 3 anvertraut oder zugänglich gemacht worden sind, nicht offenbaren oder verwerten (Bankgeheimnis)." (§ 38 Abs 1 Satz 1 BWG)

Sie verpflichten sich die Rechte und Pflichten wie nachfolgend beschrieben einzuhalten: Das Bankgeheimnis bedeutet einerseits die

- **Verpflichtung**, keine Auskünfte über Produkte von Kund:innen und über sonstige Tatsachen kommerzieller oder technischer Art, die aufgrund der Geschäftsverbindung bekannt werden, zu geben und andererseits die

- **Berechtigung**, solche Auskünfte Dritten gegenüber zu verweigern, soweit nicht in Einzelfällen durch das Gesetz eine Auskunftspflicht statuiert wird.

Das Bankgeheimnis erstreckt sich auf alle Tatsachen, die dem geheimhaltungspflichtigen Personenkreis ausschließlich aufgrund seines:ihres Berufes bzw. seiner:ihrer Funktion bekannt werden, wie z.B. auf das Bestehen eines Kontos, Buchungen auf demselben, Kreditgewährung bzw. Ablehnung eines Kreditantrages, usw.

Im Zweifel werden alle Tatsachen aus dem Geschäftsbereich der Kund:innen als geheimhaltungsbedürftig behandelt.

5.3 Datengeheimnis - §6 DSG

Im Zuge Ihres Dienstverhältnisses erhalten Sie Kenntnis von **personenbezogenen Daten** der Kund:innen und von Arbeitskollegen:innen sowie von Daten, welche die technische Infrastruktur und den strukturellen Aufbau von Anwendungen betreffen (nachfolgend gemeinsam als „Daten" bezeichnet). Sie verpflichten sich personenbezogene Daten aus Datenverarbeitungen, die Ihnen ausschließlich aufgrund Ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich worden sind[1],

<u>geheim</u> zu halten,

soweit kein **rechtlich zulässiger Grund für eine Übermittlung dieser Daten** besteht (Datengeheimnis). Rechtlich zulässige Gründe für die Beschränkungen des Datengeheimnisses können nur die Einwilligung der betroffenen Person, deren lebenswichtige Interesse, ein öffentliches Interesse[2], das berechtigte Interesse eines anderen aufgrund eines Vertrages oder einer rechtlichen Verpflichtung sein.

[1] unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten wie dem **<u>Bankgeheimnis</u>**
[2] nur aufgrund einer gesetzlichen Grundlage

Sie dürfen Daten nur aufgrund einer ausdrücklichen Anordnung ihres Dienstgebers (und jeweiligen Vorgesetzten) übermitteln. Dies erfolgt insbesondere durch mündliche oder schriftliche Aufgabenzuteilung.

Es ist untersagt, Daten an unbefugte Empfänger:innen innerhalb und außerhalb des Unternehmens zu übermitteln oder sonst zugänglich zu machen sowie sich unbefugt Daten zu einem anderen als dem zur rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu beschaffen oder zu verarbeiten.

Die gesetzliche Verpflichtung zur Wahrung des Bank- und Datengeheimnisses dauert während der Zugehörigkeit zum Unternehmen sowie auch nach dem Ausscheiden aus dem Unternehmen fort.

5.4 Verletzung von Geschäfts- und Betriebsgeheimnissen

Im Rahmen der Ausübung Ihrer beruflichen Tätigkeit erhalten Sie **Kenntnis über Geschäfts- und Betriebsgeheimnisse**[3]. Alle diese Informationen sind absolut vertraulich zu behandeln und unterliegen den Bestimmungen des österreichischen und europäischen Wettbewerbsrechts[4].

5.5 Folgen einer Verletzung der Geheimnispflicht

Die schuldhafte **Verletzung des Bankgeheimnisses kann zu Schadenersatzforderungen** gegenüber der Bank und unter Umständen Regress an **Mitarbeiter:innen** führen. Es können einzelne Personen **strafrechtlich** belangt werden[5] und es drohen Verwaltungsstrafen (ua. Zwangsstrafen durch FMA, potenziell Konzessionsentzug) sowie zivilrechtliche Unterlassungsansprüche.

Das Datenschutzgesetz sieht bei Verletzungen des Datengeheimnisses **Geldstrafen** vor (Verwaltungsübertretung[6]), unter Umständen sogar **Freiheitsstrafen**[7]. Im Strafgesetzbuch werden ebenfalls bestimmte unrechtmäßige Verarbeitungen von Daten[8] **auch ohne Personenbezug** mit **Geld- und Freiheitsstrafen** bedroht[9].

Wer als Bedienstete:r eines Unternehmens **Geschäfts- oder Betriebsgeheimnisse[10], die ihm im Zuge des Dienstverhältnisses anvertraut oder sonst zugänglich geworden** sind, während der Geltungsdauer des Dienstverhältnisses unbefugt anderen zu Zwecken des

---

[3] Geschäfts- oder Betriebsgeheimnisse sind Tatsachen kommerzieller oder technischer Art, die nur einer bestimmten und begrenzten Anzahl von Personen bekannt und anderen nicht oder nur schwer zugänglich sind, nach dem Willen des Berechtigten nicht über den Kreis der Eingeweihten hinausdringen sollen und an deren Geheimhaltung der Unternehmensinhaber ein wirtschaftliches Interesse hat

[4] ua. § 11 Bundesgesetz gegen den unlauteren Wettbewerb („UWG")

[5] §101 BWG, Geld oder Freiheitsstrafe

[6] § 62 DSG

[7] § 63 DSG

[8] sowohl personenbezogenen als auch nicht personenbezogenen Daten und Programme

[9] Insbesondere die Tatbestände „Widerrechtlicher Zugriff auf ein Computersystem", „Verletzung des Telekommunikationsgeheimnisses", „Missbräuchliches Abfangen von Daten", „Betrügerischer Datenverarbeitungsmissbrauch", „Missbrauch von Computerprogrammen oder Zugangsdaten" sowie „Datenfälschung" und „Datenbeschädigung" kommen in Frage.

[10] § 11 UWG

Wettbewerbes mitteilt, ist vom Gericht mit **Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen** zu bestrafen.

Die **gleiche Strafe trifft den**, der Geschäfts- oder Betriebsgeheimnisse, deren Kenntnis er durch oben genannte Mitteilungen oder durch eine gegen das Gesetz oder die guten Sitten verstoßende eigene Handlung erlangt hat, **zu Zwecken des Wettbewerbes unbefugt verwertet oder an andere mitteilt**. Zusätzlich kann eine Klage auf Unterlassung und Schadenersatz folgen[11].

6. DATENSCHUTZ IM HOMEOFFICE

Der:die Dienstnehmer:in ist verpflichtet, die gesetzlichen und betriebsinternen Regelungen zur Umsetzung des Datenschutzes und der Datensicherheit zu beachten und anzuwenden. Vertrauliche Daten, Informationen und Gespräche sind vom Dienstnehmer:in so zu sichern bzw. zu führen, dass Dritte einschließlich der Familienangehörigen, keinen Zugang und keine Kenntnis erhalten. Die zur Verfügung stehenden Schutzmechanismen wie unter anderem E-Mail-Klassifizierungen („unified labelling") und Einschränkungen der Berechtigungen auf Daten und Dokumente sind zu nutzen.

Sollten im HomeOffice keine Möglichkeiten einer Aktenvernichtung bestehen (z.B. Ofen, Shredder der gültige Industrienormen für hohen Schutzbedarf erfüllt), sind vertrauliche Unterlagen im Büro zu entsorgen.

7. DATENSCHUTZ BEI BESUCHERTAGEN

Unser Unternehmen nimmt regelmäßig am Vorarlberger Zukunftstag „Ich geh mit" teil. An diesem Tag wird den Kindern von Mitarbeiter:innen die Möglichkeit geboten, die Arbeitswelt „Raiffeisenbank" näher kennenzulernen. Alle in diesen Besuchertag involvierten Dienstnehmer:innen sind in besonderem Maße dazu angehalten, ihrer Geheimhaltungspflicht entsprechend dafür Sorge zu tragen, dass den Besuchern keine geheimnisrelevanten Informationen offengelegt werden (Ausdrucke, einsehbare Bildschirme, …).

8. VERWENDUNG VON DRUCKERCODE BEI ZENTRALEN DRUCKERINSELN

Für die Einhaltung des Datenschutzes und Datensicherheit ist bei Verwendung der Drucker bei der Druckerinsel ausnahmslos ein Code für den Papierausdruck zu verwenden.

Die Anleitung zur Einrichtung des Druckercodes ist in diesem IMS Beitrag enthalten.

[11] §13 UWG

9. AKTENVERNICHTUNG UND ALTPAPIERENTSORGUNG

Die Aktenvernichtung und Altpapierentsorgung im Unternehmen selbst werden von einem externen zertifizierten Partner durchgeführt.

In die Altpapiercontainer darf kein für die Aktenvernichtung bestimmte, geheimnisrelevante Informationen gelangen.

Für Daten-, Bank- und Geschäftsgeheimnis relevante Daten ist nachstehende Vorgehensweise einzuhalten:

- Die Vernichtung der ausgedruckten Daten ist von der jeweiligen Abteilung zum Datenvernichtungscontainer zu bringen und in den Einwurfschlitz zu werfen.
- Dadurch wird ein Zugriff auf diese Daten bestmöglich verhindert.
- Die Vernichtung sonstiger Datenträger wie Folien, Disketten, CDs etc. erfolgt durch die Nachbearbeitung der RLB Geschäftsbereich ORG/IT (Auftrag im Ticketsystem ist zu erstellen).

10. DATENSCHUTZVERLETZUNGEN

Datenschutzverletzungen sind **unrechtmäßige** oder **unbeabsichtigte Datenvernichtungen, -verluste, -veränderungen, unbefugte -offenlegungen oder sonstige Datenverarbeitungen** (nachfolgend kurz „Datenschutzverletzung"). Es ist unerheblich, ob die Datenschutzverletzung mit Vorsatz, unbewusst, fahrlässig oder durch (technische) Fehler während der Datenverarbeitung verursacht wird. Unwesentlich ist auch, welche Art von Datenträger betroffen ist oder welche Art der Verarbeitung zur Verletzung geführt hat.

Merksatz: **Bei einer Datenschutzverletzung kommt es zu Unregelmäßigkeiten, welche die Verfügbarkeit, Vertraulichkeit oder Integrität von personenbezogenen Daten betreffen.**

Beispiele

- Datenvernichtung (Verfügbarkeitsverletzung)
- Schädigung von personenbezogenen Daten (Integritätsverletzung)
- Datenverlust (Verfügbarkeitsverletzung)
- Unbefugte Offenlegung beziehungsweise unbefugter Zugang (Vertraulichkeitsverletzung)

Sofern keine personenbezogenen Daten betroffen sind, liegt auch keine Datenschutzverletzung vor. Eine Verletzung der IT-Sicherheit ohne Personenbezug ist keine Datenschutzverletzung. Dennoch ist höchste Sorgfalt geboten, da Geschäfts- und Betriebsgeheimnisse zu wahren sind und andere interne Meldepflichten an den:die Informationssicherheitsbeauftragte:n ausgelöst werden können.

Risiken für die Rechte und Freiheiten natürlicher Personen entstehen potenziell aus einer Verarbeitung, die zu einem physischen, materiellen oder immateriellen Schaden führen kann[12].

Sie verpflichten sich, potenzielle und tatsächliche Datenschutzverletzungen über die intern bereitgestellten Kommunikationskanäle zu melden.

Eine Meldung bringt für den:die Mitarbeiter:in keine zusätzlichen Sanktionen mit sich, wirkt sogar entlastend.

11. AUFBEWAHRUNG VON E-MAILS UND GESCHÄFTSBRIEFEN

Grundsätzlich müssen Geschäftsbriefe[13] zumindest 7 Jahre[14] aufbewahrt[15] werden, darüber hinaus noch so lange, als sie für ein anhängiges gerichtliches oder behördliches Verfahren benötigt werden[16]. Gesetzliche Bestimmungen können diese Frist verlängern[17].

Geschäftsbriefe sind beispielsweise Aufträge samt Ergänzungen, Auftragsbestätigungen, schriftliche Verträge, Versandanzeigen, Lieferscheine, Frachtbriefe, Rechnungen, Gutschriften, Unterlagen über Zahlungsflüsse, Reklamationen sowie Zahlungsbelege.

Keine Geschäftsbriefe sind allgemeine Informationen, Werbematerial (Prospekte, Postwurfsendungen), Glückwunschschreiben oder ähnliches. Private Korrespondenz fällt nicht unter die Aufbewahrungspflicht.

Sofern für einen **Geschäftsbereich konkrete Ablagevorschriften für bestimmte Dokumenttypen bestehen, sind diese einzuhalten**.

Sie **verpflichten sich dazu, die internen Aufbewahrungs- und Löschvorgaben einzuhalten** und bei **Unsicherheiten** die **Unterstützung** der Fachexperten einholen.

[12] ErwGr. 75, 76 DSGVO
[13] Geschäftsbriefe sind alle Schriftstücke, die ein unternehmensbezogenes Geschäft betreffen
[14] ab Ende des Geschäftsjahres, in dem der Geschäftsbrief empfangen oder gesendet wurde
[15] § 212 Unternehmensgesetzbuch
[16] in dem das Unternehmen Parteistellung hat
[17] (beispielsweise müssen Geschäftsbriefe, die Aufzeichnungen und Unterlagen über Grundstücksgeschäfte enthalten, 22 Jahre aufbewahrt werden