Raiffeisen Landesbank Vorarlberg

BETRIEBSVEREINBARUNG

Über ein Hinweisgebersystem

abgeschlossen zwischen der	**Raiffeisen Landesbank Vorarlberg** mit Revisionsverband eGen Rheinstraße 11, 6900 Bregenz
sowie dem	**Betriebsrat** der Raiffeisen Landesbank Vorarlberg mit Revisionsverband eGen

Version: 1.0 – Redigiert für die Veröffentlichung auf der Website
Gültig ab: 01.12.2020

INHALTSVERZEICHNIS

1. VORWORT

Grundlage dieser Betriebsvereinbarung ist die „Rahmenbetriebsvereinbarung über die Verwendung personenbezogener Arbeitnehmerdaten" sowie gesetzliche Notwendigkeiten[1]. Mit diesen gesetzlichen Bestimmungen werden Kreditinstitute und Wertpapierfirmen zur Schaffung eines Hinweisgebersystems verpflichtet, welches den Mitarbeitenden unter Wahrung der Vertraulichkeit ihrer Identität ermöglicht, betriebsinterne Verstöße an eine geeignete Stelle zu melden.

Welche Verstöße durch das zuständige Gremium behandelt werden, lässt sich in aktueller geltender Fassung auf der Hinweisgeberplattform nachvollziehen (Hinweistext) und wird in Punkt 3 Definitionen „Hinweisgebersystem" beschrieben.

Der Einsatz eines umfassenden Hinweisgebersystems dient als ein Signal, dass rechtlich und ethisch einwandfreies Verhalten eingefordert wird sowie Maßnahmen ergriffen werden, um Vermögens- und Imageschäden von der Bank abzuwenden.

Der Dienstgeber sowie der Betriebsrat sind sich bewusst, dass sich derzeit umfangreiche unionsrechtliche Vorgaben zum Schutz von Hinweisgebern im Entstehungsprozess befinden. Diese werden insbesondere im Rahmen der durchzuführenden Datenschutz-Folgenabschätzung sowie in zukünftigen Anpassungen des Prozesses berücksichtigt.

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

2. GELTUNGSBEREICH

Diese Betriebsvereinbarung gilt personell für alle von den abschließenden Betriebsräten vertretenen Arbeitnehmer der Raiffeisenlandesbank Vorarlberg Waren- und Revisionsverband registrierte Genossenschaft mit beschränkter Haftung, im Folgenden als Arbeitnehmer zusammengefasst.

Als Arbeitnehmer werden im Sinne dieser Betriebsvereinbarung alle natürlichen Personen bezeichnet, die von der Unternehmensleitung verschieden sind. Dies ist im Sinne des § 36 ArbVG zu verstehen. Davon sind auch Personen erfasst, die aufgrund ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen angesehen sind, wie Heim-/ und Leiharbeitnehmern und Personen, die zu Schulungs- und Ausbildungszwecken langfristig beschäftigt werden.

Sachlich gilt diese Betriebsvereinbarung für die gänzliche oder auch nur teilweise automatisierte Verarbeitung personenbezogener Daten in diesem IKT-System[2], sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Darüber hinaus sollen die Bestimmungen auch für mündliche Meldungen an die genannten Ansprechpartner gemäß Punkt 5 „Ansprechpartner" Geltung finden.

[1] § 99 lit g BWG, § 98 WAG, § 40 FM-GwG sowie der unionsrechtlichen Vorgaben
[2] Definition siehe Rahmenbetriebsvereinbarung „Informations- und Kommunikationstechnik"

3. DEFINITIONEN

Hinweisgeber
Hinweisgeber sind Personen, die zu wirtschaftskriminellen Handlungen, Verstößen gegen gesetzliche und aufsichtsrechtliche Vorgaben sowie schadensrelevanten Verstößen gegen betriebsinterne Vorgaben in einem Unternehmen aus ihrer Verantwortung heraus oder aufgrund eines Gewissenkonflikts Meldungen tätigen. Hinweisgeber genießen besonderen Schutz. Bei vorsätzlich getätigten falschen Beschuldigungen drohen jedoch Sanktionen (§297 StGB).

Hinweisgebersystem / Whistleblowing-Plattform
Das Hinweisgebersystem dient grundsätzlich nur der Meldung von Verstößen, welche verpflichtend gesetzlich durch den Arbeitgeber bearbeitet werden müssen[3]. Das System dient der Risikofrüherkennung bei gleichzeitigem Schutz der involvierten Personen sowie der Vorbeugung krimineller Handlungen und Verstößen gegen gesetzliche und aufsichtsrechtliche Vorgaben.

4. ZIELSETZUNG

Die gegenständliche Betriebsvereinbarung regelt die Nutzung des Hinweisgebersystems sowie die Verwendungsmöglichkeiten der verarbeiteten Daten.

Die nachfolgenden Bestimmungen sollen gewährleisten, dass allen Hinweisen auf wirtschaftskriminelle Handlungen, Verstößen gegen gesetzliche und aufsichtsrechtliche Vorgaben, die von Arbeitnehmern gemeldet werden, in nachvollziehbarer Weise nachgegangen wird. Zudem soll die Einhaltung der aufsichtsrechtlichen Anforderungen[4] sowie der arbeits- und datenschutzrechtlichen Bestimmungen (Schutz des Hinweisgebers und der beschuldigten Personen sowie deren personenbezogene Daten) gewährleistet werden.

Der Arbeitgeber betont, dass bei einem begründeten Verdacht bevorzugt eine Meldung an den Vorgesetzten getätigt und über diesen eine Lösung für einen Verstoß oder ein Problem gefunden werden soll. **Basierend auf einer Kultur des offenen Umgangs mit Problemen, soll die Meldung an den Vorgesetzten sowie ein offener Umgang mit Problemen und Missständen gefördert werden.**

[3] Derzeit gegen die Bestimmungen der in § 70 Abs. 4 Bankwesengesetz angeführten Bundesgesetze, gegen die Bestimmungen Verordnung (EU) Nr. 575/2013 (CRR), gegen Bestimmungen der Verordnung (EU) Nr. 600/2014, gegen die Bestimmungen der Verordnung (EU) 2015/847 und §40 FM-GwG, gegen Bestimmungen des Wertpapieraufsichtsgesetzes (jeweils in der geltenden Fassung) sowie gegen auf Grund dieser angeführten Bundesgesetze und Verordnungen erlassenen weiterführenden Verordnungen oder Bescheide. Das Hinweisgebersystem dient auch der Umsetzung von Gesetzen, die aufgrund der Richtlinie (EU) 2019/1937 erlassen werden (Festlegung von Mindeststandards zum Schutz von Personen, die Verstöße gegen Unionsrecht melden)
[4] gemäß EBA/GL/2017/11 in der geltenden Fassung

5. ANSPRECHPARTNER - GREMIUM FÜR DIE RLBV

Leiter der WAG Compliance Abteilung
Leiter der Innenrevision
Leiter der Unternehmens-Compliance

Das Gremium ist für die Bearbeitung der Hinweise verantwortlich. Das Gremium unterliegt einer strikten Geheimhaltungspflicht in Bezug auf die in ihrer Verantwortung liegenden Sachverhalte. Für alle anderen gemeldeten Sachverhalte besteht eine eingeschränkte Geheimhaltungspflicht des Gremiums. Diese Sachverhalte werden nach freiem Ermessen der Gremiumsmitglieder und eines einstimmigen Beschlusses samt Dokumentation an die zuständigen Personen innerhalb der Organisation zur weiteren Bearbeitung weitergeleitet. Die Empfänger sind ebenso zur Wahrung der Vertraulichkeit verpflichtet, worauf das Gremium anlässlich der Übermittlung an die Empfänger besonders hinweist. Näheres zum Ablauf findet sich unter Punkt 6.2.

6. DAS HINWEISGEBERSYSTEM IM DETAIL

6.1 Kommunikationswege

Dem Hinweisgeber stehen verschiedene Kommunikationswege zur Verfügung.

Hinweisgeberplattform
Im Informationsmanagementsystem des Dienstgebers ist ein zentraler, gut sichtbarer Verweis auf die Hinweisgeberplattform zu platzieren. Das Hinweisgebersystem bietet die Möglichkeit zur anonymen oder offenen Meldung.

Weitere Einmeldemöglichkeiten
Meldungen können postalisch (Adresse lt. Hinweisgeberplattform) und anonym an die unter Punkt 5 genannten Personen und den Ombudsmann erfolgen. Es besteht zudem eine Einmeldemöglichkeit per E-Mail.

6.2 Ablauf

1. Der Hinweis wird vom Hinweisgeber im Hinweisgebersystem als **offener Hinweis oder geschützter Hinweis (anonym) erfasst**. Es ist für den meldenden Mitarbeiter nicht erforderlich, einen Beleg für einen Verstoß vorzulegen, allerdings sollte er über ein ausreichendes Maß an Gewissheit verfügen, dass ein hinreichender Grund für die Einleitung einer Untersuchung vorliegt[5].
   Richtet sich ein Hinweis gegen ein Mitglied des Gremiums, ist dieser Hinweis nach Möglichkeit zwecks Wahrung der Vertraulichkeit außerhalb des Hinweisgebersystems vollinhaltlich samt Kontaktaufnahmemöglichkeit direkt an ein unbefangenes Mitglied des Gremiums oder den Ombudsmann zu melden. Dieses unbefangene Mitglied hat umgehend die notwendigen Maßnahmen zu setzen.

2. Der Hinweisgeber kann auf der Plattform oder schriftlich verlangen, dass die **Informationen von Beginn an in anonymisierter Form dem Gesamtvorstand** vorgelegt werden. Sofern dies geschieht, soll der Vorstand der RLBV bzw. die Geschäftsführung der

[5] Ein dementsprechender Hinweis findet sich auch auf der Hinweisgeberplattform informiert

Tochterunternehmen in der Regel zuerst mit dem Gremium Kontakt aufnehmen und das weitere Vorgehen absprechen, da dieses für die Bearbeitung des Hinweises hauptverantwortlich ist. Bis zu einer Abstimmung mit dem Gremium und der Klärung des weiteren Vorgehens hat der Vorstand über die Meldung grundsätzlich Verschwiegenheit zu wahren.

3. Das **Gremium dokumentiert alle Schritte**, die im Zusammenhang mit der Beschuldigung gesetzt werden, insbesondere Protokolle der internen Abstimmungen. Die Unterlagen und Protokolle dürfen nur den einzelnen Gremiumsmitgliedern zugänglich sein, eine **Weitergabe von Informationen bzw. Daten darf nur einstimmig erfolgen**.

4. Der Hinweisgeber erhält, sofern er seine Identität bzw. eine eigene Kommunikationsmöglichkeit bekannt gibt, innert einer Woche eine **Empfangsbestätigung** sowie innert drei Monaten eine Information über die in die Wege geleiteten Schritte. Sofern möglich und zweckdienlich, erhält der Hinweisgeber den **Bearbeitungsabschluss** mitgeteilt. Er hat jedoch kein Recht auf Bekanntgabe des **Bearbeitungsergebnisses**.

5. Mit der Einleitung von Ermittlungen sind Beschuldigte von einem Mitglied des Gremiums **grundsätzlich über die Anschuldigungen zu informieren**, sofern der Ermittlungserfolg durch eine Information des Beschuldigten nicht gefährdet ist.

6. Das **Gremium entscheidet gemeinsam und einstimmig** über die weitere Vorgangsweise. Im Ausnahmefall kann bei der Abwesenheit eines Gremium-Mitgliedes und bei Gefahr in Verzug auf die Abstimmung verzichtet werden. Sofern eine Meldung nicht weiter zu verfolgen ist, wird diese **Entscheidung jedenfalls gemeinsam sowie einstimmig getroffen und dokumentiert**. Die Mitglieder des Gremiums sind berechtigt, mit dem Hinweisgeber in geeigneter Form in Kontakt zu treten, um z.B. Rückfragen zu stellen.

7. Spätestens nach Abschluss der Untersuchungen wird der **Beschuldigte durch ein Mitglied des Gremiums über die Existenz der Meldung informiert**, sofern dadurch nicht die Durchführung eines Gerichts- oder Verwaltungsverfahrens vereitelt wird. Eine Information unterbleibt gänzlich in den Fällen, in denen das Gremium entschieden hat, eine Meldung mangels Substanz nicht weiter zu verfolgen oder eine Meldung abzulehnen, weil sie nicht im Einklang mit den Meldesachverhalten des Hinweisgebersystems ist. Den Mitgliedern des Gremiums obliegt die Verantwortung für die ordnungsgemäße Abwicklung und revisionssichere Dokumentation ihrer Beratungen.

8. Das Gremium sowie auch der Ombudsmann können jederzeit, nach eigenem Ermessen und einstimmigem Beschluss, sofern es als erforderlich angesehen wird und den Ermittlungsverlauf nicht behindert, ein Organ des Unternehmens über Meldungen und Ermittlungsergebnisse informieren. Vor weiterführenden Untersuchungen und Kontaktaufnahme mit Gerichten oder Behörden ist der Gesamtvorstand vom Gremium jedenfalls zu benachrichtigen (sofern dadurch der Ermittlungserfolg nicht gefährdet ist).

9. **Anlassbezogen berichtet das Gremium an den Gesamtvorstand** über die eingegangenen Meldungen soweit möglich ohne Personenbezug (Anzahl und Art der Hinweise wie beispielsweise ob es sich um offene oder anonyme Hinweise gehandelt hat, mitsamt einer kurzen Fallbeschreibung / Sachverhalt, Status / Ergebnis der Bearbeitung, gegebenenfalls auch abgewiesene Hinweise samt Abweisungsbegründung). Der Bericht erfolgt nicht

hinweisgeberbezogen, sondern bezieht sich ausschließlich auf den Hinweis selbst und seine Inhalte.

7. GEHEIMHALTUNG DER IDENTITÄT DES HINWEISGEBERS

In mehrfacher Hinsicht wird die gesetzlich geforderte Geheimhaltung der Identität des Hinweisgebers[6] sichergestellt. Wie in Punkt 6 und Punkt 8.2 ausgeführt, wird die Vertraulichkeit der Daten der involvierten Personen gewahrt und die Identität des Hinweisgebers gemäß dem need-to-know Prinzip geheim gehalten.

Zudem besteht die Möglichkeit anonymer Meldungen über die Whistleblowing-Plattform. Es wird darauf hingewiesen, dass bei Inanspruchnahme dieser Möglichkeit auch darauf geachtet werden soll, keine Informationen über den Hinweisgeber selbst bei der Sachverhaltsdarstellung preiszugeben.

Entsprechend den technischen und organisatorischen Maßnahmen gemäß Anlage A ist sichergestellt, dass eine Rückverfolgbarkeit und Identifizierung des Hinweisgebers verunmöglicht wird. Zudem wird anhand der weiterführenden Dokumentation und periodischen Prüfung in der Datenschutz-Folgenabschätzung sichergestellt, dass Anpassungen zum Schutz der Identität des Hinweisgebers gemäß dem sich laufend fortbildenden Stand der Technik vorgenommen werden.

8. SCHUTZ FÜR DIE MITARBEITENDEN[7]

Die Vertraulichkeit der personenbezogenen Daten des Hinweisgebers[8] sowie aller in der Meldung angeführten, bzw. beschuldigter Personen wird durch die Geheimhaltungspflicht des Gremiums und des Ombudsmannes gewahrt. Daten des hinweisgebenden Mitarbeiters sowie der beschuldigten Person werden betriebsintern und betriebsextern durch dokumentierte technische und organisatorische Maßnahmen entsprechend der Anlage A geschützt.

Ausnahmen von der Vorgehensweise im Regelfall (Vertraulichkeit der Daten des Hinweisgebers und aller involvierter Personen):

I. wenn der Dienstgeber Anzeige erstattet und der Hinweisgeber **zwingend als Zeuge für das Verfahren benötigt** wird oder im Falle eines Strafverfahrens gegen die Bank, in dessen Folge die Vertraulichkeit der Daten des Hinweisgebers aufzuheben ist.
II. Wenn sich aufgrund **eines erheblichen Verdachtes oder im Zuge von Ermittlungen** ergibt, dass der Hinweisgeber vorsätzlich falsche Beschuldigungen[9] angestellt hat. In diesem Fall kann die Offenlegung des Hinweisgebers durch das Gremium und den Betriebsrat erwirkt werden.

Hinweisgeber, die Verstöße im Sinne dieser Betriebsvereinbarung melden oder Hinweise an die FMA weiterleiten, dürfen deswegen weder[10]

[6] insbesondere § 99g Abs 3 Z 4 BWG, § 98 Abs 3 Z 3 WAG, §40 FM-GwG
[7] § 99 g Abs 3 Z 2 BWG
[8] und damit auch die Information, wer der Hinweisgeber ist
[9] wie zumindest Vergeltungsmaßnahmen, Diskriminierung oder anderen Arten von Mobbing
[10] §98 Abs 4 WAG

I. benachteiligt, insbesondere nicht beim Entgelt, beim beruflichen Aufstieg, bei Maßnahmen der Aus- und Weiterbildung, bei der Versetzung oder bei der Beendigung des Arbeitsverhältnisses, oder
II. nach strafrechtlichen Vorschriften verantwortlich gemacht werden,

es sei denn, die Meldung ist vorsätzlich unwahr abgegeben worden.

8.1 Schutz vor Vergeltungsmaßnahmen

Schutz vor Vergeltungsmaßnahmen, Diskriminierungen, anderen Arten von Mobbing, Viktimisierung[11]:

Im Falle der Benachteiligung eines Mitarbeiters kann sich dieser jederzeit an den Betriebsrat wenden, welcher weitere Maßnahmen veranlasst und beratend zur Seite steht. Sollte ein Personalgespräch mit dem Betroffenen gesucht werden, muss der Betriebsrat informiert werden. Zudem muss bei der Einladung auf die Kritikalität des Gesprächs, sowie auf die Möglichkeit, den Betriebsrat[12] hinzuzuziehen, hingewiesen werden.

Sollte eines der Mitglieder des Gremiums von einer etwaigen Benachteiligung Kenntnis erlangen, hat dieser den Betriebsrat zu informieren. Gegebenenfalls kann zusätzlich auch unverzüglich der Vorstand oder der Aufsichtsrat informiert werden.

8.2 Schutz der personenbezogenen Daten[13]

In allen Fällen mit hinreichendem Anfangsverdacht werden Ermittlungen eingeleitet. Ermittlungen werden – entsprechend dem Need-to-know-Prinzip – mit größtmöglicher Vertraulichkeit unter Hinzuziehung des jeweilig notwendigen Personenkreises geführt. Eingehende Meldungen und die dazugehörige Dokumentation des Gremiums werden gemäß den internen Ablagestandards und dem Löschkonzept aufbewahrt. Eine darüberhinausgehende Aufbewahrung ist nur zulässig, wenn und solange die Meldung für die Durchführung eines Gerichts- oder Verwaltungsverfahrens oder für disziplinäre Maßnahmen erforderlich ist oder im Einzelfall eine hohe Wahrscheinlichkeit von nachfolgenden Verfahren besteht. Das Sicherheitskonzept findet sich im Anhang A.

Weitere Rechte, die nach datenschutzrechtlichen Vorgaben gebühren, werden entsprechend der Rahmenbetriebsvereinbarung gewahrt. Sollte anhand einer Einzelfallbeurteilung unter Hinzuziehung des Datenschutzbeauftragten ein Recht nur eingeschränkt gewährt werden, wird die Begründung für die Nichterfüllung dokumentiert abgelegt. Beispielsweise kann das „Recht auf Auskunft" gemäß der DSGVO[14] eingeschränkt werden, sofern es eine laufende Untersuchung gefährdet.

Eine Grundrechtsprüfung, Risikoanamnese sowie getroffene Maßnahmen hinsichtlich eines Eingriffs in die Rechte und Freiheiten der Betroffenen finden sich in der DSFA[15], welche bei Abschluss dieser Detailbetriebsvereinbarung vorliegt. Die DSFA unterliegt einem periodisch durchzuführenden Review durch den Datenschutzbeauftragten. Das Ergebnis der Prüfung sowie allfällige Empfehlungen zu Änderungen an der Datenverarbeitung oder den Rahmenbedingungen werden dem Dienstgeber und dem Betriebsrat nachweislich zur Kenntnis gebracht.

[11] Schädigung durch kriminelles Handeln, zum „Opfer" machen
[12] Recht auf Beistand
[13] Ua. § 99g Abs 3 Z 3 BWG
[14] Art. 15 der Verordnung (EU) 2016/79 (Datenschutz-Grundverordnung)
[15] „Datenschutz-Folgenabschätzung – Hinweisgebersystem"

Daten werden nur für folgende, bestimmte Zwecke benutzt:

I. Im Rahmen der Aufklärung und Verfolgung wirtschaftskrimineller Handlungen und gesetzlicher Verstöße,
II. zur Sicherung der Interessen und zum Schutz der personenbezogenen Daten des Hinweisgebers, insbesondere seiner Anonymität und dem Schutz vor Nachteilen;
III. zum Schutz des Beschuldigten, insbesondere vor Nachteilen;
IV. zur Wahrung der Interessen der Bank sowie zur Wahrung berechtigter Interessen Dritter, insbesondere deren Risiko- und Schadensminimierung sowie für dienstrechtliche Maßnahmen;
V. zur technischen Wartung des Hinweisgebersystems. Die Systemadministratoren haben keinen direkten Zugriff auf die Daten, allerdings kann eine Kenntnisnahme von Daten nicht gänzlich ausgeschlossen werden. Die Administratoren absolvieren eine besondere Datenschutz-Schulung, in welcher auf die Sensibilität der vertraulichen Informationen hingewiesen wird.

Eine Verarbeitung der Daten zu anderen Zwecken ist verboten.

9. RECHTE DES BETRIEBSRATES

Die Informations- bzw. Anhörungsrechte des Betriebsrates vor dem Ausspruch eventueller arbeitsrechtlicher Konsequenzen bleiben hiervon unberührt.

Dem Betriebsrat stehen die ihm gesetzlich zustehenden Kontroll- und Informationsrechte entsprechend der Rahmenbetriebsvereinbarung zu. Der technische Verantwortliche für den Betrieb des jeweiligen Systems ist gegenüber dem Betriebsrat hinsichtlich der technischen Aspekte auskunftspflichtig. Jede Änderung des Systems ist durch den Betriebsrat zustimmungspflichtig und wird entsprechend nach Freigabe in der Anlage A aktualisiert. Ausgenommen davon sind System-Aktualisierungen, welche die vorliegende Betriebsvereinbarung nicht tangieren und den vereinbarten Umfang der Verarbeitungen nicht überschreiten.

10. DATENKATEGORIEN UND RECHTSGRUNDLAGE

Das Hinweisgebersystem kann Kontaktdaten, elektronische Identifikationsdaten, AML- und Compliance-Daten, Anmeldedaten, Personal-Ordnungsnummern, Deskriptionsdaten, Namen bzw. Bezeichnungen, den Inhalt der Meldung, die Grundlage der Meldung, spezielle Finanzdaten, meldepflichtige Daten, Daten über strafrechtliche Verurteilungen und Straftaten sowie Daten zu Beurteilungen und Einschätzungen verarbeiten und enthalten. Entsprechend der Rahmenbetriebsvereinbarung handelt es sich hierbei um Kategorie A, B und Kategorie D-Daten. Die Verarbeitung der personenbezogenen Daten erfolgt auf der Rechtsgrundlage „rechtliche Verpflichtungen“[16], die Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten aufgrund einer ausdrücklichen gesetzlichen Verpflichtung[17] sowie allgemein im Rahmen dieser Detailbetriebsvereinbarung und ansonsten im Rahmen der berechtigten Interessen des Unternehmens an der Einhaltung interner Compliance- und Governance Vorgaben. Die Daten müssen den gesetzlichen Verpflichtungen entsprechend bei Verdacht der

[16] Art. 6 Abs 1 lit c DSGVO
[17] § 4 Abs 3 Z 1 DSG iVm § 99 g Abs 1 BWG bzw. iVm § 98 Abs 1 WAG, §40 FM-GwG

Begehung von Straftaten verarbeitet und aus Beweisgründen gesichert werden, hierbei erfolgt die Verarbeitung aufgrund überwiegender Interessen des Verantwortlichen oder von Dritten[18].

11. WIRKSAMKEITSBEGINN UND GELTUNGSDAUER

Diese Betriebsvereinbarung tritt mit Unterzeichnung in Kraft und gilt bis zum 30.11.2024. Sollte weder die vorliegende Betriebsvereinbarung einvernehmlich gekündigt werden noch eine Beendigung aus wichtigem Grund erfolgen, ist hiermit ein wiederholter Abschluss ohne Zutun der Parteien bis 30.11.2028 vereinbart.

Die Betriebsvereinbarung kann jederzeit in beidseitigem Einverständnis ergänzt werden[19]. Diese Betriebsvereinbarung wird durch Abrufmöglichkeit im Intranet gehörig kundgemacht.

Für den Betriebsrat

Für die Raiffeisenlandesbank Vorarlberg

[18] Art. 6 Abs 1 lit f DSGVO

[19] insbesondere der einen integrierenden Bestandteil dieser Betriebsvereinbarung bildende Anhang A kann nach gemeinsamer Abstimmung zwischen Betriebsrat und Dienstgeber, ohne dass es einer Änderung der BV bedürfte, aktualisiert werden

12. ÄNDERUNGSHISTORIE

In der Änderungshistorie werden für die Leser des Dokuments die wesentlichen Änderungen im Laufe der Versionierung beschrieben. Dies soll eine Hilfestellung sein, damit bei neuen Versionen nicht das gesamte Dokument gelesen werden muss, sondern nur die geänderten Inhalte:

13. ANHÄNGE

13.1 Anhang A - Sicherheitskonzept

Die Daten werden über eine Weboberfläche per E-Mail (SMTP) an eine Lotus Notes Datenbank übermittelt. Das Logging für die Website ist deaktiviert (Nutzer, IP Adresse, Uhrzeit sind für die Subdomäne ausgeschaltet und werden somit nicht protokolliert). Der Transport der Daten erfolgt über eine mittels TLS Verschlüsselung geschützte https-Website.

Die Mail-Maske wird anschließend zusammengestellt, wobei ansonsten keine Meldungen im Cache oder in ähnlichen Anwendungen gespeichert werden. Der Notes SMTP Server sendet vom Absender die Meldung per E-Mail an die hinterlegte Whistleblower-E-Mail-Adresse, wobei der Transportweg von Notes Client zu Notes Server verschlüsselt erfolgt (Asynchrone Verschlüsselung mit zumindest 630 Bit). Die jeweilige Datenbank ist verschlüsselt (die Server-ID ist verschlüsselt), diese kann zwar kopiert aber nicht geöffnet werden. Die jeweilige Lotus Notes Benutzer-ID ist ebenfalls durch eine zwei Faktor-Authentifizierung (Karte plus PIN) geschützt.

Sonstige Maßnahmen zur eindeutigen Identifizierung sind nicht installiert. Auf die in der E-Maildatenbank hinterlegten Daten kann nur mit einer entsprechenden Infrastruktur wie Notes Client oder Notes Server und der notwendigen Berechtigung (Authentifizierung) zugegriffen werden. Eine Änderung der Berechtigungen darf nur durch einen einstimmigen Auftrag durch das Gremium beauftragt werden. Auf die Datenbank sind nur das zur Vertraulichkeit verpflichtete Gremium und die technisch verantwortlichen Dienstleister, welche einer besonderen Geheimhaltungsverpflichtung unterliegen, zugriffsberechtigt.

Die technisch verantwortlichen Dienstleister erhalten eine spezielle Datenschutz-Schulung, die vom Datenschutzbeauftragten durchzuführen ist.