Regelwerkversion	**3-0**	Vertraulichkeitsklassifikation	**intern**
gültig ab	**01.10.2021**	Eigner	**IT**
		Betroffene Prozesse	**-**
		verfügbare Sprachen	**DE, FR, IT**

Betroffene Divisionen / Bereiche	**Konzernbereiche, Infrastruktur, M&P Personenverkehr, Immobilien, und Konzerngesellschaften**
Spezifische Empfänger / Verteiler	**LIDI-R, A2, A20**
Ersatz für	**Regelwerkversion 2-0**
Zuordnung	**K 018.4**

Umgang mit IT-Arbeitsmitteln und Geschäftsdaten

Inhalt

Änderungsverzeichnis

Version	Kapitel	Änderung
3-0	3	Integration der Weisung K 400.16 Informationsklassifizierung
2-0	3.1	Anpassungen für Azure Information Protection
1-0		Erstausgabe, Ersatz für K 400.5, K 400.8, K 400.9, K 400.33, K 400.43, K 400.44

1. Allgemeines

1.1. Ausgangslage, Ziele

Ein sorgfältiger Umgang mit IT-Arbeitsmitteln und Geschäftsdaten ist ein zentrales Element für den Schutz von Personendaten, vertraulichen und internen Informationen sowie für den Schutz der Informatiksysteme und damit des gesamten Betriebs.

1.2. Geltungsbereich (Unternehmen, Anwender / Funktion)

Diese Vorgaben gelten für sämtliche Personen, welche IT-Arbeitsmittel und Geschäftsdaten der SBB AG oder der SBB Cargo AG nutzen.

2. Meine Arbeitsmittel

Den SBB Mitarbeitenden werden für die Erfüllung ihrer Arbeitsaufgaben grundsätzlich IT-Arbeitsmittel zur Verfügung gestellt. Mitarbeitende oder Mitarbeitende von Lieferanten und Partnern können unter bestimmten Auflagen aber auch eigene IT-Arbeitsmittel verwenden. Dies wird als «Bring your own Device» oder kurz «BYOD» bezeichnet.

2.1. Umgang mit IT-Arbeitsmitteln

Du gehst mit den von der SBB zur Verfügung gestellten IT-Arbeitsmitteln sorgfältig um und schützt sie vor Schaden und Verlust.

Du lässt deine IT-Arbeitsmittel im Betriebszustand nicht unbeaufsichtigt. Beim Verlassen des Arbeitsplatzes sperrst du deine IT-Arbeitsmittel. Du verleihst deine IT-Arbeitsmittel mit Geschäftsdaten der SBB nicht an Dritte.

PC und Notebook kannst du jederzeit sperren durch Drücken der **Windows + L-Taste** oder (**Control+Alt+Delete, Enter**). Auch Tablet und Smartphone kannst du mit der Ausschalttaste sperren.

2.2. Passwörter

Du hältst deine persönlichen Passwörter geheim und gibst sie nicht an andere Personen weiter. Dein Passwort gibst du unbeobachtet vor den Augen Dritter ein. Geschäftliche Passwörter dürfen nicht für private Dienste verwendet werden.

Die höchste Sicherheit bietet ein langes Passwort. Überlege dir also eine zufällige Aneinanderreihung von Wörtern. Diese Wortkombination kannst du dir gut merken und sie bereitet Hackern am meisten Schwierigkeiten.

Weitere Informationen zum Umgang mit dem SBB Password findest du hier.

2.3. Nutzungsbestimmungen für spezifische IT-Arbeitsmittel

Für bestimmte IT-Arbeitsmittel und IT-Dienste gibt es zusätzliche Nutzungsbestimmungen. Die entsprechenden Vorgaben erhältst du mit dem Gerät oder beim Aufschalten des jeweiligen Dienstes. Zudem sind die IT-Arbeitsmittel durch technische Massnahmen geschützt. Diese sogenannten

„Gerätepolicies“ stellen einen Mindestschutz sicher (z.B. verlangt ein Smartphone zwingend einen Code und wird nach einer bestimmten Zeit gesperrt).

Technische Schutzmassnahmen darfst du nicht entfernen oder umgehen.

Beim Zugriff auf Geschäftsdaten mit privaten Geräten („BYOD“), welche nicht durch die SBB verwaltet werden, stellst du folgenden Mindestschutz sicher:

- Gerätepasswort mit mindestens 4 Ziffern
- Auto-Lock nach 5 Minuten
- Geräteverschlüsselung
- iOS: Löschung aller Daten (komplette Rückstellung auf Werks-einstellungen) nach zehnmaliger Falscheingabe des Gerätepassworts.
- Android: Löschung aller Daten im SBB Arbeitsbereich nach zehnmaliger Falscheingabe des Gerätepassworts.

Hier findest du alle Informationen zum Umgang mit mobilen Geräten; insbesondere bei Eintritt, Übertritt und internem Wechsel, Austritt, Geräte-Austausch und beim Einsatz eines privaten Geräts («BYOD»).

Weitere Nutzungsbedingungen beim Einsatz von privaten Geräten («BYOD») für den Zugriff auf Office 365 findest du hier.

Die «Mobile Device Services» («MDS») berechtigen SBB Mitarbeitende, mit von SBB Informatik freigegebenen mobilen Geräten E-Mails, Kalender-einträge, Kontakte, Notizen und Aufgaben zu synchronisieren sowie mit den entsprechenden Apps («Password», «Mitarbeitendenportal» etc.) auf das SBB Unternehmensnetzwerk zuzugreifen.

Du findest die Nutzungsbedingungen für den MDS-Dienst hier.

Alles zum Thema Work Smart/Telearbeit findest du auf der entsprechenden Informationsseite.

3. Umgang mit Informationen

3.1. Klassifikation

Geschäftsdaten umfassen Daten und Informationen, welche in Zusammenhang mit der SBB stehen. Dazu gehören Daten der SBB, von Kunden, Mitarbeitenden, Lieferanten und Geschäftspartnern.

Die Daten können beispielsweise in Form von Office-Dokumenten, E-Mails, Papierunterlagen, Personal-Dossiers und Rechnungen vorliegen.

Die nachfolgenden Klassifikationsvorgaben gelten ebenfalls für strukturierte Daten, beispielsweise Datenbanken in Geschäftsanwendungen.

Der Dokumenten Owner ist verantwortlich für den gesamten Lebenszyklus eines Dokuments und ist verpflichtet, die korrekte Ablage, Aufbewahrung und Archivierung zu veranlassen. Der Dokumenten Owner stellt sicher, dass die Zugriffsrechte entsprechend der Vertraulichkeit eingeschränkt sind.

Dokumenten Owner ist insbesondere, wer ein Dokument erstellt, auf einer Geschäftsablage der SBB ablegt oder Anpassungen an einem solchen Dokument vornimmt. Bei Anpassungen muss die Klassifikation überprüft und gegebenenfalls angepasst werden.

Bei der SBB gibt es für Dokumente und Geschäftsdaten die folgenden Klassifikationsstufen:

C1 Öffentlich sind Daten, die für die Öffentlichkeit erstellt wurden. Dazu gehören beispielsweise der Fahrplan, Verkaufsprospekte oder Medienmitteilungen.
Ein Vermerk auf dem Dokument ist nicht notwendig.

C2 Intern sind Daten, welche für den internen Gebrauch und ausgewählte weitere Adressaten bestimmt sind. Dazu gehören interne Weisungen, das Telefonverzeichnis oder die Dienstadresse. Solche Informationen sind im Rahmen des Offenheitsprinzips für folgenden Empfängerkreis mit Leserechten zugänglich:

- interne Mitarbeitende der SBB
- Lernende und Praktikanten der SBB
- externe Mitarbeitende
- Mitarbeitende von Beteiligungsgesellschaften mit einer Mehrheitsbeteiligung der SBB
- unpersönliche User SBB

Ein Vermerk „C2 - Intern“ auf dem Dokument wird empfohlen, ist aber nicht zwingend.

C3 Vertrauliche Daten sind besonders schützenswerte Daten. Dazu gehören Finanzreportings, Risikodokumentationen, Dokumentationen kritischer Technologien, Protokolle von VR, KL und GL-Sitzungen und besonders schützenswerte Personendaten.
Auf vertrauliche Dokumente gehört zwingend der Vermerk „C3 - Vertraulich“ und du schränkst den Zugriff auf den notwendigen Empfängerkreis ein.

Die Verwendung von vertraulichen Daten für eigene, kommerzielle, oder öffentliche Zwecke oder zur Nutzung für Forschung und Lehre ist nur mit schriftlicher Zustimmung der SBB (Dokumentenowner nach Absprache mit dem zuständigen Rechtsdienst) gestattet.
Informationen, die einer besonderen Geheimhaltungspflicht unterliegen (z.B. nachrichtendienstliche Dokumente), gelten als «persönlich vertraulich». Deren Dokumentenlenkung unterliegt speziellen Bestimmungen und die Mitarbeitenden sind an die entsprechenden Geheimhaltungspflichten gebunden.

Die Office Applikationen erleichtern dir die Klassifikation von Dokumenten und tragen dazu bei, dass vertrauliche Informationen besser geschützt werden. Mit nur einem Knopfdruck wird das Dokument klassifiziert und der Vermerk automatisch auf dem Dokument angebracht.

Weiterführende Informationen zum Thema Klassifizierung von Dokumenten findest du hier.

In Office Applikation klassifizierst du vertrauliche Dokumente grundsätzlich mit der Klassifizierungsstufe „C3.2 – SBB verschlüsselt“.

Bei „persönlich vertraulichen“ Dokumenten und Emails wird die höchste Stufe „C3.3 Persönlich verschlüsselt“ empfohlen. Damit kann der Zugriff zusätzlich, unabhängig vom Ablageort, dank der Verschlüsselung auf einen sehr eingeschränkten Empfängerkreis reduziert werden.

C3.3 ist auch die richtige Klassifizierung bei einem Austausch von vertraulichen Dokumenten und Emails mit externen Stellen ohne SBB Account.

In Ausnahmefällen, z.B. falls es in der Zusammenarbeit zu technischen Problemen kommt, darf vorübergehend, mit der entsprechenden Sorgfalt, die Stufe „C3.1 – Unverschlüsselt“ verwendet werden. Der Zugriff ist jedoch zwingend auf die notwendigen Personen einzuschränken.

3.2. Vertraulichkeit und Geheimhaltung

Du behandelst Geschäftsdaten der SBB mit der notwendigen Sorgfalt. Auch interne Daten gehören nicht an die Öffentlichkeit. Innerhalb der SBB tauschen wir als «intern» klassifizierte Daten jedoch offen aus und nutzen diese zur übergreifenden Zusammenarbeit zum Wohle der SBB (sogenanntes Offenheitsprinzip).

Der sorgfältige Umgang mit Geschäftsdaten ist ein wichtiges Element des Verhaltenscodex der SBB.

Du schützt vertrauliche, geschäftliche Inhalte von Gesprächen, Papierdokumenten, mobile Datenträger sowie auf deinem Bildschirm und bewahrst diese vor unberechtigtem Zugriff.

Einen Sichtschutzfilter für dein Notebook bekommst du im ICT-Serviceportal. Wähle Bestellportal und gib den Suchbegriff «Sichtschutz» ein. Du erhältst eine Auswahl von Sichtschutzfiltern für verschiedene Notebooktypen.

Nutze für vertrauliche Gespräche, wenn möglich, einen abschliessbaren Fokusraum. Ein Zugabteil und/oder Restaurants sind keine Orte für vertrauliche Telefongespräche.

Lasse Papierdokumente und mobile Datenträger nicht offen herumliegen und trage insbesondere ausserhalb der Arbeitsräume Sorge zu ihnen.

3.3. Datenablage und Aufbewahrung

Geschäftsdaten legst du auf den von der SBB zur Verfügung gestellten Services ab (Sharepoint, OneDrive for Business, DMS, Filer etc.). Private Cloud-Services (private Dropbox oder iCloud) sind nicht zulässig für die Ablage von Geschäftsdaten. Vertrauliche Dokumente legst du grundsätzlich in einer Ablage mit entsprechend eingeschränkten Zugriffsrechten ab.

Physische Dokumente mit der Klassifizierung „C2 – Intern“ sind in einem geschützten Bereich (Zugang nur mit Badge/Schlüssel) aufzubewahren.

Physische Dokumente mit der Klassifizierung „C3 -Vertraulich“ sind verschlossen (z.B. abgeschlossener Schrank) in einem geschützten Bereich aufzubewahren.

Du findest Informationen zur Datenablage in Sharepoint, OneDrive for Business und DMS auf der Seite des ICT-Workplace.

Du findest Informationen zum Schutzzonenkonzept im Security Handbuch der SBB und im zugehörigen Schutzzonenkonzept.

3.4. Versand von Unterlagen

Für den geschäftlichen Austausch von Nachrichten (Mails oder Sofortnachrichten) verwendest du die offiziellen SBB-Systeme des IT-Workplace. Du leitest geschäftliche Nachrichten nicht an private Mail- oder Messengerdienste weiter. Ein physischer Versand von vertraulichen Dokumenten wird nicht empfohlen, hat jedoch ausschliesslich eingeschrieben in verschlossenen Umschlägen zu erfolgen.

Vertrauliche Informationen überträgst du grundsätzlich verschlüsselt. Sie dürfen ohne Zustimmung des Dokumentenowners nicht an Externe weitergeleitet werden.

Weiterführende Vorgaben zum Umgang mit der elektronischen Kommunikation und zum Umgang mit sozialen Medien finden du hier: Verhaltensgrundsätze Elektronische Kommunikation und Social Media Guide

3.5. Mobile Datenträger

Mobile Datenträger sind nur für öffentliche Daten einzusetzen (z.B. grosses Firmen-Video, welches die Speicherkapazität überschreitet). Geschäftsdaten mit der Klassifikation «intern» oder «vertraulich» gehören auf die dafür vorgesehenen Geschäftsablagen (z.B. SharePoint oder das geschäftliche OneDrive). Zum Datenaustausch ist die Freigabefunktion zu verwenden.

Du kannst Geschäftsdaten nicht nur SBB intern, sondern auch mit Dritten mittels Sharepoint teilen. Wie das klappt, erfährst du in dieser Anleitung auf der Seite des ICT-Workplace.

3.6. Drucken

Vertrauliche Dokumente dürfen nur mit der Funktion „Vertraulicher Druck“ oder mittels „FollowMe Printing“ ausgedruckt werden.

3.7. Entsorgung

Physische Dokumente und Speichermedien sind fachgerecht in den dafür vorgesehenen Behältern zu entsorgen.

4. Sicherheitsrelevante Vorkommnisse

Verlust oder Diebstahl von Geräten mit Geschäftsdaten, relevante Vorfälle im Bereich Informationssicherheit und allfällige Verstösse im Bereich Datenschutz meldest du umgehend dem ICT Service Desk
(Telefon **+41 51 220 30 40**).

5. Software und Apps

Du verwendest zu Geschäftszwecken grundsätzlich Software, welche von der SBB beschafft und lizenziert wurde.

Wenn du nicht von der SBB bereitgestellte Software zu Geschäftszwecken verwendest (sowohl auf SBB Geräten wie auch auf BYOD-Geräten), so bist du dafür verantwortlich, dass die Software auch für geschäftliche Zwecke genutzt werden kann und korrekt lizenziert ist.

Du stellst zudem sicher, dass die Software auf einem aktuellen Stand gehalten wird und verfügbare Security-Updates umgehend installiert werden.

Zusätzliche Softwareprodukte können über das ICT-Serviceportal bestellt werden.

6. Private Nutzung, Persönlichkeitsrechte und Überwachung

6.1. Private Nutzung

ICT-Mittel, welche von der SBB zur Verfügung gestellt werden, sind primär für die geschäftliche Nutzung vorgesehen. Die Mitarbeitenden dürfen diese in angemessenem Rahmen und Umfang auch für private Zwecke nutzen.

Du greifst nicht auf Inhalte mit rechtswidrigen oder anstössigen Inhalten zu (sexistisch, rassistisch, extremistisch, pornographisch, unethisch, diffamierend).

Der Zugriff kann durch Arbeitsanweisungen im Rahmen der Verhältnismässigkeit eingeschränkt oder verboten werden, wenn die Person zum Beispiel mit Überwachungsfunktionen betraut ist.

Deine unmittelbar vorgesetzte Person kann die Nutzung privater Applikation oder des Internets im Rahmen der Verhältnismässigkeit einschränken oder verbieten, wenn ein begründeter Verdacht oder Gewissheit besteht, dass die private Nutzung das zulässige Mass überschreitet oder auf rechtswidrige respektive anstössige Inhalte zugegriffen wird.

Käufe und Bezüge von Dienstleistungen mit Mobile-Abonemmenten z.B. per Mobilerechnung, kostenpflichtige SMS oder SMS-Pay für private Zwecke sind nicht erlaubt.

Detaillierte Informationen zur Bezahlung mit Smartphone (über ein Mobilabonemment der SBB) findest du im Beitrag: mit SBB Smartphone bezahlen.

6.2. Persönlichkeitsrechte und Überwachung

Zur Sicherstellung des Betriebs ist es teilweise notwendig, dass SBB IT-Arbeitsmittel überwacht werden.

Bei entsprechenden Überwachungs- und Auswertungsmassnahmen wird sichergestellt, dass alle gesetzlichen und internen Vorgaben, sowie die Vereinbarungen mit den Sozialpartnern eingehalten werden. Zudem wird sichergestellt, dass die Massnahmen einen möglichst geringen Eingriff in die Persönlichkeitsrechte darstellen.

Bei Überwachungsmassnahmen berücksichtigt die SBB das Verhältnismässigkeitsprinzip und verwendet nur diejenigen Auswertungs- und Überwachungsmassnahmen, welche für den angestrebten Zweck den geringsten Eingriff in die Persönlichkeitsrechte darstellen.

Weiterführende Informationen findest du in der Weisung K 155.1.

IT

sig. Marcus Griesser
CISO

IT

sig. Daniel Wild
Security and Risk Manager

Regelwerkversion	**3-0**	Vertraulichkeitsklassifikation	**intern**
Gültig ab	**15.11.2021**	Eigner	**IT**
		Betroffene Prozesse	**Steuerung Informatik**
		Verfügbare Sprachen	**DE**

Betroffene Divisionen / Bereiche	**Konzernbereiche, Infrastruktur, M&P Personenverkehr, Immobilien, und Konzerngesellschaften**
Spezifische Empfänger / Verteiler	**LIDI-R: A2, A20**
Ersatz für	**Regelwerkversion 2-0**
Zuordnung	**K 018.4**

Homologation von Hard- und Software

Änderungsverzeichnis

Version	Kapitel	Änderung
3-0	Alle	Anpassung an neue Organisation
2-0	Alle	Wechsel von K-IT zu IT. Ersatz von R K durch K.
1-0	Alle	Erstausgabe: Erstausgabe: Ersatz für R Z 400.1 Ausgabedatum: 01.01.2007

1. Allgemeines

1.1. Ausgangslage, Ziele

Das Ziel dieser Regelung sind verbindliche Vorgaben für die Homologation von Hard- und Software vor dem Anschluss ans SBB-Datennetz.

1.2. Geltungsbereich

Die Regelung ist verbindlich für die Mitarbeitenden der SBB, sowie für die Mitarbeitenden von der SBB geführten und voll konsolidierten Konzerngesellschaften der SBB AG.

Die Regelung gilt zusätzlich für Mitarbeitende von Drittfirmen, die Dienstleistungen zugunsten der SBB erbringen.

Die Regelung gilt für Hard- und Software, welche in Netzwerkbereichen der SBB betrieben werden, welche durch das Netzwerkauthentisierungssystem (NAS/NAC) überwacht werden.

Die Regelung gilt nicht für den Standard-IT-Arbeitsplatz SBB und nicht für Inhalte des IT-Warenkorbes (Hard- und Software).

1.3. Übergeordnete und zugehörige Dokumente

Übergeordnete Regelungen:

K 018.4 Informationssicherheitspolitik der SBB

K 400.20 IT-Governance

1.4. Begriffe und Abkürzungen

Anwendungssoftware	Eine Anwendungssoftware ist eine Software, die angewendet wird, um eine nützliche oder gewünschte Funktion auszuführen (zB. Bildbearbeitung, Textverarbeitung, Tabellenkalkulation etc.)
Benutzer	Mitarbeitende weiblichen und männlichen Geschlechts der in 1.2 genannten Organisationen.
Beteiligungsgesellschaften der SBB	Gesellschaften, bei denen SBB AG 50% und mehr der Anteile halten.
Betriebsprozess	Der Betriebsprozess ist in einem Betriebskonzept /-handbuch festzulegen. Er umfasst eine Darstellung der Betriebsorganisation, der Ansprechpartner und deren Verantwortlichkeiten, das Hardware Lifecycle Management, Produkt Management, Mengengerüste, Testkonzepte, sowie die Prozesse Incident-, Problem-, Change-, Release-, Configuration-, Financial- und Capacity-Management.
Homologation	Unter Homologation wird eine Verträglichkeitsprüfung von IT-Mittel (Hardware, Software) bei deren Beschaffung verstanden. Je nach IT-Mittel sind unterschiedliche

	Aspekte zu prüfen. Darunter fallen Datenkommunikations-, , Security- sowie Betriebsaspekte. Damit soll sichergestellt werden, dass die IT-Landschaft der SBB die Geschäfts-prozesse möglichst störungsfrei und sicher unterstützen.
IT-Warenkorb	Der standardisierte IT-Warenkorb, welcher durch IT im Intranet SBB publiziert wird.
NAS/NAC	Das Netzwerkauthentisierungssystem der SBB, welches unerlaubter Hardware den Zugriff auf das SBB-Datennetz unterbindet.
Software	Anwendungs- und Systemsoftware
Standard IT-Arbeitsplatz	Der Standard IT-Arbeitsplatz der SBB. Die Publikation dieses Arbeitsplatzes erfolgt im IT-Warenkorb.
Systemsoftware	Systemsoftware umfasst das Betriebssystem und die System- und Hilfsprogramme, die den technischen Betrieb ermöglichen, aber noch keinen Anwender-bezogenen Nutzen bringen. Dazu gehören z.B. auch Werkzeuge zur Softwareerstellung.
Tochtergesellschaften der SBB	Gesellschaften bei denen SBB 100% der Anteile halten.

2. Vorgabe

2.1. Grundsatz

Es werden nur Geräte zur Homologation zugelassen, wenn die damit auszuführenden Geschäftstätigkeiten nicht mit einem Standard-IT-Arbeitsplatz ausgeführt werden können.

2.2. Definition von Gerätetypen

Im Rahmen der Homologation werden die folgenden Gerätetypen unterschieden:

Gerätetyp 1:
- Hardware mit unveränderbarem Betriebssystem (ROM-basiert)
- Hardware ohne Betriebssystem

Gerätetyp 2:
- Hardware mit veränderbarem Betriebssystem (inkl. Software)

2.3. Definition von Homologationsarten

Für die Homologation des Gerätetyps 2 werden die folgenden Homologationsarten unterschieden:

Einzelgerät: Homologation eines einzelnen Gerätes, inklusive installierter Software und Konfiguration und dokumentiertem Betriebsprozess. Die Homologation gilt für genau 1 Gerät (1 Stück).

Geräteserie: Homologation eines einzelnen Gerätemodells, inklusive installierter Software und dokumentiertem Betriebsprozess. Die Homologation

gilt für mehrere Geräte (n Stück), welche alle dieselbe Software installiert haben, gleich konfiguriert sind und gemäss einem einheitlichen Betriebsprozess betrieben und gewartet werden.

2.4. Homologationsprozess

Die folgenden Homologationsschritte müssen erfolgreich durchlaufen werden, damit eine Homologation abgeschlossen werden kann:

Homologations-stellen / Typ	I-ET-TC (Netzverträglichkeit Sicherheitsaspekte)	IT (DSRV-TE) (Sicherheitsaspekte)	IT DSRV-SMIB (Betriebsprozess, Zonenowner)
Gerätetyp 1	JA	Nein	Nein
Gerätetyp 2 (Einzelgerät / Geräteserie)	JA	JA	JA

2.5. Bestellung

Zur Beantragung einer Homologation ist folgendes Formular auszufüllen:

- Formular Homologation

2.6. Abschluss

Als Bestätigung der erfolgreichen Homologation erfolgt die Aufnahme des Gerätes in der Asset-Management-Database (AMDB). Mit dem Eintrag in die AMDB wird auch die Freischaltung im NAS/NAC ausgelöst.

2.7. Homologationsdauer

Die Geräte gelten als homologiert, sobald sie in der AMDB eingetragen sind. Die Homologation gilt während maximal 4 Jahren. Nach Ablauf der Homologationsdauer werden die Geräte gesperrt und es muss ggf. eine neue Homologation beantragt werden.

2.8. Kontrolle

Überprüfungen durch die Homologationsstellen gemäss Kapitel 2.4 sind jederzeit möglich. Geräte, welche die Homologationsvorgaben nicht mehr erfüllen bzw. bei Nichteinhalten der dokumentierten Betriebsprozesse kann die Homologation durch SBB Cyber & Privacy entzogen werden und die Geräte können im SBB-Datennetz gesperrt werden.

3. Abhängigkeit zu anderen Regelungen

Die Homologationsvorgaben für die Aufnahme von Produkten in den IT-Warenkorb werden in K 400.31 Homologation von Hard- und Software des IT-Warenkorbes geregelt.

4. Disziplinarische Massnahmen

Verstösse gegen diese Regelung werden disziplinarisch verfolgt.

IT	IT
sig. Jochen Decker	sig. Marcus Griesser
CIO	CISO

Regelwerkversion	**3-0**	Vertraulichkeitsklassifikation	**intern**
gültig ab	**01.06.2021**	Eigner	**RC**
		Betroffene Prozesse	**----**
		verfügbare Sprachen	**DE, FR, IT**

Betroffene Divisionen	**Konzernbereiche, Infrastruktur, M&P Personenverkehr, Immobilien, und Konzerngesellschaften**
Spezifische Empfänger / Verteiler	**LIDI-R: A2 / A3 / A20**
Ersatz für	**Regelwerkversion 2-0 und K 040.0**
Zuordnung	**K 014.1**

Datenschutz

Inhalt

Änderungsverzeichnis

Version	Kapitel	Änderung
3-0		Komplette Überarbeitung inkl. Integration Regelung K 040.0
2-0		Komplette Überarbeitung
1-0		Erstausgabe

1. Allgemeines

1.1. Ausgangslage, Ziele

Vorliegende Regelung Datenschutz basiert auf den Werten des Code of Conducts der SBB sowie auf der Datenschutzstrategie der SBB. Sie wird auf Basis der «Fachführung RC Personendaten», GR KL Anhang 1 K 011.2 erlassen.

Die Regelung Datenschutz bezweckt die Festlegung der Organisation und Verantwortlichkeiten betreffend die Umsetzung der anwendbaren rechtlichen und regulatorischen Vorgaben im Bereich Datenschutz.

Die vorliegende Regelung bestimmt die Grundsätze, welche bei der Bearbeitung von Personendaten zu beachten sind. Ausserdem legt sie die Aufgaben, Kompetenzen und Verantwortlichkeiten des Datenschutzmanagementsystems fest.

1.2. Geltungsbereich

Vorliegende Regelung befasst sich ausschliesslich mit dem Bearbeiten von Daten über Kunden, Mitarbeitende und weitere Personen, kurz: Personendaten. Die Regelung regelt dagegen nicht die Bearbeitung von rein technischen Daten, d.h. Daten ohne jeglichen Personenbezug.

Die Regelung gilt für sämtliche Mitarbeitende der SBB AG und der SBB Konzerngesellschaften, an denen die SBB AG direkt oder indirekt eine Mehrheitsbeteiligung hält (im Folgenden gemeinsam als SBB bezeichnet), soweit mit den Konzerngesellschaften nichts anderes vereinbart wurde. Organisatorische und strukturelle Vorgaben dieser Regelung werden durch die Konzerngesellschaften sinngemäss umgesetzt. Die Konzerngesellschaften richten sich dabei nach den Vorgaben der Fachstelle Datenschutz. Sie erhalten von dieser analoge und auf ihre Grösse und ihr Risikoprofil angepasste Vorgabedokumente und Prozesse der SBB zur Umsetzung und Anwendung.

1.3. Übergeordnete und zugehörige Regelungen

Dieser Regelung übergeordnet ist das Organisationsreglement (OGR) und der Verhaltenskodex SBB (Code of Conduct). Die Regelung konkretisiert die Vorgaben betreffend den Compliance-Bereich Datenschutz gemäss der Compliance-Policy (K 014.1).

Untergeordnete Regelwerke sind betreffend Daten von Mitarbeitenden die Vereinbarungen zum Persönlichkeits- und Datenschutz (K 122.1 und K 122.2) sowie die Vorgaben betreffend die personenbezogene Auswertung von Mitarbeiterdaten (K 155.1).

Konkretisierendes Regelwerk für den Umgang mit Kundendaten sind die Ausführungsbestimmung («Vertrauen in Umgang mit Kundendaten») zu dieser Regelung. Die Datenschutzklassifikationen werden in der Regelung Informationsklassifikation (K 400.16) geregelt.

1.4. Begriffe und Definitionen

Personendaten:

Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.

Bearbeiten:

Das Bearbeiten von Personendaten umfasst jeglichen Umgang mit Personendaten unabhängig von den angewandten Mitteln und Verfahren, insb. das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren und Vernichten.

Datenbearbeitungsverzeichnis (DBV):

Das Datenbearbeitungsverzeichnis (DBV) bildet eine Sammlung der Personendatenbearbeitungen der SBB und ihre Beschreibung (insb. Bearbeitungszweck).

Datenschutz-Folgenabschätzung (DSFA):

Die DSFA ist eine vertiefte Risikoanalyse für Datenbearbeitungen. Die Verantwortlichen müssen sie bei geplanten Bearbeitungstätigkeiten, die ein potenziell hohes Risiko für die Betroffenen nach sich ziehen könnten (z.B. Diskriminierung, Rufschädigung oder Identitätsdiebstahl), vorab durchführen.

Datenschutzerklärung:

Mit einer Datenschutzerklärung wird die betroffene Person über die Bearbeitung ihrer Daten informiert (die Erklärung kann insbesondere über das Internet erfolgen).

Datenschutzrisikoregister:

Von den Datenschutzberatern wird ein Register geführt, das die Datenschutzrisiken den Risk Ownern zuweist und entsprechende Kontrollen und Massnahmen zur Risikobewältigung ausweist.

Datenschutzvorfall:

Personenbezogene Daten gehen verloren, werden gelöscht oder vernichtet, werden verändert oder Unbefugten zugänglich gemacht.

Datentyp:
Alle Daten der SBB sind nach verschiedenen Datentypen strukturiert (vgl. Datenstrategie SBB).

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB):

Der EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter) beaufsichtigt Bundeorgane und Privatunternehmen in Bezug auf ihre Bearbeitungen von Personendaten.

Modell der Drei Linien:

Vom Institute of Internal Auditors anerkanntes und von der SBB genutztes Modell zum Management von Risiken. Das Modell der 3 Linien ist in der Compliance Policy beschrieben und definiert die Compliance Governance-Grundsätze. Die 1. Linie bildet das operative Management. Sie trägt die Verantwortung für die Einhaltung der Datenschutzvorgaben sowie der damit verbundenen Risiken. Die 2. Linie (Fachstelle Datenschutz) dient der Überwachung und Unterstützung der 1. Linie. Die interne Revision der SBB (REV) prüft und bewertet als 3. Linie die Wirksamkeit und Effizienz des DSMS in seiner Gesamtheit.

2. Grundsätze des Datenschutzes und Datenschutz-Managementsystem

2.1. Grundsätze des Datenschutzes

Zielsetzung des Datenschutzes ist der Schutz der Persönlichkeit und nicht der Schutz der Daten. Durch Beachtung der nachfolgenden Grundsätze des Datenschutzes kann eine rechtmässige Datenbearbeitung sichergestellt und die Privatsphäre der Betroffenen geschützt werden.

- **Rechtmässigkeit:**
  Die Bearbeitung der Personendaten muss in Übereinstimmung mit der geltenden Rechtsordnung erfolgen. Die Verantwortlichen stellen sicher, dass für ihre Bearbeitungen die rechtlichen Grundlagen (Einwilligungen, Vertragserfüllung, überwiegende Interessen oder eine spezifische gesetzliche Grundlage) vorhanden sind.

- **Transparenz:**
  Die von der Bearbeitung betroffenen Personen müssen erkennbar, umfassend und verständlich über die Beschaffung ihrer Daten, den genauen Bearbeitungszweck sowie die Bearbeitungsart informiert werden, und zwar bevor die Bearbeitung erfolgt. Die Verantwortlichen stellen sicher, dass ihre Bearbeitungen nicht ohne Kenntnis der Betroffenen oder für andere als bei der Beschaffung angegebene Zwecke erfolgt.

- **Verhältnismässigkeit:**
  Personendaten dürfen nur verhältnismässig bearbeitet werden. Die Verantwortlichen stellen insbesondere sicher, dass nur nur diejenigen Personendaten

bearbeitet werden, welche für die Erreichung des Bearbeitungszwecks erforderlich und geeignet sind. Eine Datensammlung "auf Vorrat" ist unzulässig (Prinzip der Datensparsamkeit). Ebenso stellen die Verantwortlichen sicher, dass Zugriffe nach dem «Need-to-Know-Prinzip» erfolgen sowie dass Personendaten gelöscht oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.

- **Treu und Glauben:**
  Personendaten dürfen nicht entgegen Treu und Glauben bearbeitet werden. Die Verantwortlichen stellen damit insbesondere sicher, dass die Bearbeitung ohne Zwang und ohne irreführende Elemente erfolgt.

- **Zweckbindung:**
  Die Verantwortlichen stellen sicher, dass die Daten ausschliesslich zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, oder gesetzlich vorgesehen ist.

- **Datenrichtigkeit:**
  Die bearbeiteten Daten müssen eine hinreichende Qualität aufweisen und behalten. Personendaten, welche bearbeitet werden, müssen richtig sein.
  Die Verantwortlichen stellen sicher, dass angemessene Massnahmen ergriffen werden, damit die Richtigkeit der Daten gewährleistet ist und Personendaten berichtigt werden können.

- **Privacy by Design und Privacy by Default:**
  Die Verantwortlichen stellen sicher, dass die Grundsätze des Datenschutzes ab Planung berücksichtigt werden (Privacy by Design), sowie dass mittels geeigneter Voreinstellungen die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist (Privacy by Default).

- **Datensicherheit:**
  Die Verantwortlichen stellen sicher, dass die bearbeiteten Daten nicht unbeabsichtigt oder unbefugt zugänglich gemacht, geändert oder vernichtet werden oder verloren gehen. Für die angemessenen organisatorischen und technischen Massnahmen zur Gewährleistung der Datensicherheit ist die Informationssicherheitspolitik der SBB (K 018.4) und folgende einschlägig.

- **Datenbearbeitung durch Dritte (bspw. externe Provider):**
  Die Verantwortlichen stellen sicher, dass
  - keine gesetzliche oder vertragliche Geheimhaltungspflicht einer Auslagerung entgegensteht,
  - der Dritte die Datensicherheit gewährleistet,
  - und in einem Vertrag geregelt ist, dass die Daten nur so bearbeitet werden, wie es die SBB selber tun dürfte.

- **Bekanntgabe von Personendaten ins Ausland:**
  Die Verantwortlichen stellen sicher, dass das Zielland der Bekanntgabe einen angemessenen Schutz gewährleistet, oder – falls dem nicht so ist - auf andere Weise ein geeigneter Datenschutz sichergestellt wird.

- **Rechte der Betroffenen:**
  Die Verantwortlichen stellen sicher, dass die Rechte der Betroffenen gewahrt werden, insbesondere dass Auskunfts-, Berichtigungs- und Löschbegehren beantwortet und umgesetzt werden können.

- **Meldepflicht von Datenschutzvorfällen:**
  Die Verantwortlichen stellen sicher, dass der Fachstelle Datenschutz so rasch als möglich ein Datenschutzvorfall gemeldet wird.

- **Datenbearbeitungsverzeichnis:**
  Die Verantwortlichen stellen sicher, dass all ihre Datenbearbeitungen im Datenbearbeitungsverzeichnis (DBV) aufgenommen werden und richtig ausgewiesen sind.

Ausführungsbestimmungen sowie Prozessvorgaben zu den vorgenannten Grundsätzen des Datenschutzes werden gemäss Ziff.6 dieser Regelung erlassen.

2.2. Datenschutz-Managementsystem (DSMS)

Über das DSMS gewährleistet die SBB die Einhaltung der Grundsätze des Datenschutzes und die Steuerungen der Datenschutzrisiken.

Das DSMS ist ein Rahmenwerk aus Vorgaben und Werkzeugen, lehnt sich an die ISO-Standards an und ist mit dem Compliance Management System von RC (CMS) sowie dem Informationssicherheitsmanagementsystem von IT (ISMS) kompatibel. Es besteht insbesondere aus folgenden Elementen:

- Gesetzliche und interne Vorgaben
- Schulungen
- Beratungen
- Gesetzesmonitoring
- Risikobewertung, Risikosteuerung
- Vorfallmanagement
- Kontakt mit Behörden
- Audits
- Berichterstattung
- Planung

Das DSMS operiert nach dem PDCA-Prinzip (Plan – Do – Check – Act) und bezweckt eine kontinuierliche Verbesserung des Datenschutzes. Durch das DSMS werden die Tätigkeiten des operativen Managements erleichtert, kontrolliert und es wird sichergestellt, dass die Datenschutzvorgaben innerhalb der SBB umgesetzt werden können.

3. Verantwortlichkeiten und Zuständigkeiten

3.1. Verwaltungsrat (VR)

Das oberste verantwortliche Organ für den Datenschutz ist der Verwaltungsrat der SBB. Der Verwaltungsrat hat die Oberaufsicht über die Gesetzes- und Regeltreue des Konzerns. Der Verwaltungsrat wird über den Compliance Bericht von Recht und Compliance regelmässig über den Stand des Datenschutzes innerhalb der SBB in Kenntnis gesetzt.

3.2. Konzernleitung (KL)

Die Konzernleitung trägt die Verantwortung, dass die Datenschutzvorgaben durch- und umgesetzt werden und die Datenschutzorganisation mit adäquaten Ressourcen ausgestattet wird.

3.3. Linienvorgesetzte und Fachführende in der Arbeitsorganisation

Die Linienvorgesetzten und die Fachführenden in der Arbeitsorganisation sind innerhalb ihres Zuständigkeitsbereiches verantwortlich, dass die Vorgaben zum Datenschutz beachtet werden. Ihnen obliegt damit die Verantwortung für die Einhaltung des Datenschutzes für den ihnen zugewiesenen Aufgabenbereich und sie tragen die damit verbundenen Risiken. Als Risk Owner sind sie für die Risiko-Identifikation in ihrem Zuständigkeitsbereich sowie für das Massnahmen-Controlling ihrer Risiken verantwortlich.

Sie haben die dafür notwendigen Prozesse zu implementieren und zu überwachen.

Sie sorgen ausserdem für die Bekanntmachung und Einhaltung der in ihrem Verantwortungsbereich geltenden gesetzlichen Vorschriften und internen Regelungen sowie dafür, dass sämtliche unter ihrem Zuständigkeitsbereich stattfindenden Datenbearbeitungen in das Datenbearbeitungsverzeichnis aufgenommen werden.

3.4. Verantwortlicher der Datenbearbeitung

Als Verantwortlicher einer Datenbearbeitung gilt, wer über Art und Umfang der Bearbeitung entscheidet, bspw. welche Daten bearbeitet werden und zu welchem Zweck.

Die Verantwortlichen der Datenbearbeitungen werden im Datenbearbeitungsverzeichnis (DBV) aufgeführt. Sie haben die Pflicht, ihre Datenbearbeitungen im DBV anzumelden und ihre registrierten Anmeldungen aktuell und richtig zu halten.

Sie sind dafür verantwortlich, dass ihre Datenbearbeitungen rechtmässig erfolgen und die Vorgaben der SBB eingehalten werden. In ihrem Zuständigkeitsbereich sind zudem sie für die Risiko-Identifikation sowie für das Massnahmen-Controlling ihrer Risiken verantwortlich.

3.5. Mitarbeitende

Sämtliche Mitarbeitenden sind innerhalb des eigenen Verantwortungs- und Zuständigkeitsbereiches für die Einhaltung der Vorgaben zum Datenschutz verantwortlich

3.6. Fachstelle Datenschutz

Die Fachstelle Datenschutz übt gestützt auf das Geschäftsreglement der Konzernleitung, Anhang 1, die Fachführung innerhalb des Konzerns aus und erlässt konzernweite Vorgaben zur Umsetzung des Datenschutzes. Gemäss dem Drei-Linien-Modell bildet sie die 2. Linie. Als solche unterstützt und berät sie den Verwaltungsrat, die Konzernleitung, die Linienverantwortlichen sowie alle mit der Umsetzung des Datenschutzes befassten Personen, ohne diesen die Verantwortung dafür abzunehmen.

Sie betreibt das Datenschutzmanagementsystem. Sie rapportiert ihre Erkenntnisse über den Gesamtzustand im Bereich Datenschutz an den Chief Compliance Officer (CCO).

Die Fachstelle Datenschutz besteht aus den Datenschutzberatern und dem Compliance Officer Datenschutz.

3.7. Datenschutzberater

Die Datenschutzberater führen ihre Aufgaben gemäss den massgebenden Bestimmungen des Datenschutzgesetzes[1]aus. Die SBB verfügt über einen oder mehrere Datenschutzberater, welche bei Recht und Compliance angesiedelt sind. Recht und Compliance ist unabhängig von der Linie und rapportiert direkt dem CEO der SBB. Die Datenschutzberater üben ihre Funktionen fachlich unabhängig und weisungsunabhängig aus.

Es ist ihnen Zugang zu sämtlichen innerhalb der SBB durchgeführten Datenbearbeitungen und den damit in Zusammenhang stehenden Dokumenten zu gewähren. Sie verfügen über ein umfassendes Auskunfts- und Einsichtsrecht in sämtliche relevante Informationen.

Die Datenschutzberater sind verantwortlich für:

- Weiterentwicklung und Umsetzung des Datenschutzmanagementsystems;
- die Erarbeitung der konzernweiten Datenschutzvorgaben und -prozesse;
- Kommunikations- und Schulungskonzepte
- Beratung;
- Gesetzes- und Rechtsprechungsmonitoring;
- Kontaktpflege zu den Aufsichtsbehörden, insbesondere zum EDÖB;
- Management des Datenschutzrisikoregisters inkl. Risikoanalyse;
- Management des DBV;
- Koordination und Bearbeitung von Auskunfts- und Löschbegehren;
- Koordination von Datenschutzverletzungen, insbesondere Meldung an Behörden und Betroffene;
- Unterstützung bei Datenschutz-Folgenabschätzungen;
- Audits;
- Rechtliche Begleitung von Gerichtsverfahren;
- Berichterstattung.

3.8. Compliance Officer Datenschutz

Ein Datenschutzberater wird gemäss den Vorgaben der Compliance Policy zum Compliance Officer Datenschutz ernannt. Der Aufgabenbereich der Funktion Compliance Officer Datenschutz ist im Pflichtenheft Compliance Officer Datenschutz geregelt. Die Aufgaben werden durch den Compliance Officer Datenschutz in Absprache mit den Datenschutzberatern erfüllt.

3.9. Datenschutzcommunity

Unter der Fachführung der Fachstelle Datenschutz besteht ein konzernweites Netzwerk aus Datenschutzmanagern sowie Legal Counsel von RC. Sie bilden die Datenschutzcommunity. Die Datenschutzcommunity stellt die Skalierung und die unité de doctrine

[1] Art. 11a Abs. 5 lit. e DSG resp. Art. 10 revDSG.

innerhalb der SBB sicher. Die Datenschutzcommunity oder Teile davon treffen sich periodisch unter der Leitung der Fachstelle Datenschutz.

Jeder Datentyp der SBB, welcher Personendaten bearbeitet, insbesondere die Typen „Privatkunde“ sowie „Mitarbeitende“, stellt mindestens einen Datenschutzmanager. Die RC Bereiche Personenverkehr, Corporate (Arbeitsrecht), Immobilien, Infrastruktur, SBB Cargo stellen mindestens je einen Legal Counsel.

Die Fachstelle Datenschutz kann die Datenschutzcommunity um weitere Mitglieder erweitern, soweit dies zur Umsetzung des Datenschutzes in der SBB notwendig ist.

3.10. Datenschutzmanager

Die Datenschutzmanager bilden für den ihnen zugewiesenen Datentyp die erste Anlaufstelle für Anliegen im Zusammenhang mit Datenschutz.

Die Datenschutzmanager haben betreffend ihren Datentyp insbesondere folgende Verantwortlichkeiten bzw. Kompetenzen:

- Beratung;
- Unterstützung der operativen Einheiten bei der Umsetzung der Datenschutzvorgaben;
- Ausarbeitung von bereichsspezifischen Vorgaben;
- Zugangsrecht zu sämtlichen durchgeführten Datenbearbeitungen und entsprechenden Dokumenten;
- Eskalationsrecht an die Datenschutzberater;
- Unterstützung der Risk Owner bei der Risikoidentifikation;
- Unterstützung der operativen Einheiten bei Fragen zum DBV und dem Risikoregister;
- Unterstützung der Fachstelle Datenschutz bei Durchführung von Schulungen und Kommunikation;
- Unterstützung der Fachstelle Datenschutz bei Durchführung von Audits.

3.11. Legal Counsel RC

Die Legal Counsel von RC unterstützen in ihrem jeweiligen Bereich oder Division die 1. Linie, die Datenschutzberater sowie die Datenschutzmanager.

3.12. Konzernfachstelle Video

Die Konzernfachstelle Video berät unter Einbezug der Fachstelle Datenschutz die einzelnen Bereiche bei der datenschutzkonformen Planung von Videoüberwachungsanlagen und erlässt Prozesse für das Aufstellen und den Betrieb von Videoüberwachungsanlagen. Die Konzernfachstelle Video ist bei Security und Transportpolizei (STP) angesiedelt und führt ein konzernweites Videoregister.

4. Umgang mit Kundendaten

Um das Vertrauen der Kunden in den Umgang der SBB mit Kundendaten zu stärken, gelten folgende Grundsätze, welche in den Ausführungsbestimmungen («Vertrauen in Umgang mit Kundendaten») konkretisiert werden:

4.1. Kunden entscheiden selbst über die Bearbeitung Ihrer persönlichen Daten.

Kunden können innerhalb des rechtlichen Rahmens die Datenbearbeitung jederzeit ablehnen beziehungsweise ihre Zustimmung dazu widerrufen oder ihre Daten löschen lassen. Sie haben immer die Möglichkeit, anonym, also ohne Erfassung ihrer Personendaten, zu reisen.

4.2. Bei der Bearbeitung von Personendaten bieten wir Kunden einen Mehrwert.

Wir nutzen Personendaten, um den Kunden entlang der Mobilitätskette Mehrwerte zu bieten (z.B. massgeschneiderte Angebote und Informationen, Unterstützung oder Entschädigung im Störungsfall). Die Kundendaten werden somit nur für die Entwicklung, Erbringung, Optimierung und Auswertung unserer Leistungen oder für die Pflege der Kundenbeziehung verwendet.

4.3. Wir verkaufen keine Kundendaten

Eine Bekanntgabe der Kundendaten erfolgt nur gegenüber ausgewählten, in unserer Datenschutzerklärung aufgeführten Dritten und nur zu den explizit genannten Zwecken. Beauftragen wir Dritte mit der Datenbearbeitung, werden diese zur Einhaltung unserer datenschutzrechtlichen Standards verpflichtet.

4.4. Wir gewährleisten Kunden Sicherheit und Schutz für ihre Daten.

Wir garantieren den sorgsamen Umgang mit Kundendaten sowie die Sicherheit und den Schutz der Daten. Wir stellen die erforderlichen organisatorischen und technischen Vorkehrungen dazu sicher.

5. Umgang mit Mitarbeitendendaten

Für den Umgang mit Mitarbeiterdaten gelten zusätzlich der GAV und die zwischen der SBB und den Sozialpartnern abgeschlossene Vereinbarung zum Persönlichkeits- und Datenschutz (K 122.1/K 122.2).

6. Ausführungsbestimmungen und Prozessvorgaben

RC-T kann Ausführungsbestimmungen und Prozessvorgaben zu dieser Regelung erlassen oder diese Kompetenz an andere Stellen delegieren.

Bereichsspezifische Ausführungsbestimmungen zu den Vorgaben dieser Regelung (insbesondere betreffend die Umsetzung der Grundsätze des Datenschutzes) können von den entsprechenden Organisationseinheiten eigenständig verfasst werden. Die Fachstelle Datenschutz muss in die Vernehmlassung der eigenständig erarbeiteten Vorgabe einbezogen werden.

7. Anhang

Die Ausführungsbestimmung «Vertrauen in Umgang mit Kundendaten» bildet integrierenden Bestandteil der vorliegenden Regelung.

RC	RC-T
sig.	sig.
Stephanie Bregy	Tobias Schnelli
General Counsel	Compliance Officer Datenschutz