Entwurf V-0.2 vom 21.08.2024

# FAGES - Good Practice Privacy - ANHANG C

# Muster Personalreglement zum betrieblichen Informations- & Datenschutz

Diese Vorlage ist den jeweiligen Gegebenheiten anzupassen, insbesondere die Bezeichnungen in eckigen Klammern [...] und die optionalen Texte in blau. Auch darf das Dokument anders betitelt werden.

## Inhaltsverzeichnis

# Allgemeine Bestimmungen

## Gegenstand und Zweck

Diese Weisung regelt die Nutzung der Informations- und Kommunikationstechnologie (ICT), im Speziellen den Gebrauch von E-Mail und Internet und die Verwendung mobiler Geräte. Gegenstand der Weisung ist zudem der verantwortungsvolle Umgang mit Informationen (insbesondere Personendaten und Passwörter).

Sie bezweckt den Schutz der Informationen vor einem Verlust der Vertraulichkeit, Zweckbindung Verfügbarkeit und Integrität.

## Anwendungsbereich

Das Reglement gilt für alle fest oder temporär angestellten Mitarbeitenden sowie externes Personal, welches die ITC-Infrastruktur des Betriebes einrichten und warten (nachfolgend bei der Erwähnung von Mitarbeitenden grundsätzlich mitgemeint). Das Reglement und hat Weisungscharakter.

## Grundlagen

Die rechtlichen Grundlagen sind:

- das Datenschutzgesetz der Schweiz (DSG)
- Verordnung über den Datenschutz (DSV)
- Arbeitsvertrag

Grundlage dieser Regeln bildet zudem der FAGES Privacy Code of Conduct.

# Verantwortung

## Datenschutzverantwortliche Person

Die [Geschäftsführung], bei dessen längeren Abwesenheit deren Stellvertretung, nimmt die Rolle als Datenschutzverantwortliche:r (nachfolgend DSV) wahr. Der / die DSV ist für die Umsetzung dieser Weisung verantwortlich und ist Ansprechstelle für Fragen und für sicherheitsrelevante Vorkommnisse, respektive die Gefährdung oder Verletzung des Datenschutzes. Sie / er ist befugt, den Mitarbeitenden Weisungen bezüglich des Datenschutzes zu erteilen.

## Mitarbeitende

Die Mitarbeitenden sind verpflichtet, die gesetzlichen Vorgaben, diese Weisung und andere interne Regelungen zu beachten anzuwenden. Sie haben die Kenntnisnahme dieser Weisung mit ihrer Unterschrift zu bestätigen.

Sie sind verpflichtet, die ihnen zur Verfügung gestellten ICT recht- und zweckmässig einzusetzen und mit den Informationen, insbesondere mit Personendaten und besonders

sorgfältig und vertraulich umzugehen. Die Mitarbeitenden melden alle sicherheitsrelevanten Ereignisse (Probleme, Vorfälle, Mängel usw.) sowie Schäden und Verlust von Hardware und Software der/dem DSV.

Als Vertraulich gelten alle als vertraulich oder gar geheim deklarierte Informationen, Passwörter, Schlüssel zu Verschlüsselungen (Ausnahme öffentliche Schlüssel), grundsätzlich alle Informationen, welche nur für den Betrieb bestimmt sind sowie besonders schützenswerte Personendaten. Personendaten dürfen ausschliesslich nur zum vorbestimmten Zweck verwendet werden.

# Datenschutz und Informationssicherheit

## Zutritts-, Zugangs- und Zugriffsschutz

Die Mitarbeitenden sorgen dafür, dass keine Unbefugten Zutritt zu den Arbeitsräumlichkeiten haben. Halten sich externe Personen in den Betriebsräumlichkeiten auf, sind Massnahmen zu treffen, die einen unbefugten Zugang zu Informationen verhindern.

Der Arbeitsplatz ist bei Abwesenheiten so zu hinterlassen, dass keine vertraulichen Dokumente und Datenträger offen zugänglich sind (Abschliessen von Türen und Verschliessen von Fenstern, Abschliessen weiterer Räume gemäss Anweisung des DSV. Ausdrucke mit vertraulichen Informationen sind aus dem Drucker zu entfernen. Selbst bei kurzer Abwesenheit (einige Minuten) ist der Arbeitsplatzrechner zu sperren, bei längerer Abwesenheit (einige Stunden) herunterzufahren.

Die Mitarbeitenden dürfen nur ihre persönlichen Benutzerkennungen oder die ihnen zugeteilten funktionellen Kennungen verwenden. Sie sind für die mit ihren Kennungen erfolgten Zugriffe verantwortlich. Der Zugriff auf Personendaten, die nicht zur Aufgabenerfüllung benötigt werden, ist verboten.

Der Verlust von Schlüsseln, Badges, Chipkarten usw. ist umgehend der oder dem DSV zu melden. Besteht der Verdacht, dass Zugangs- oder Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden,  ist die oder der DSV umgehend zu informieren.

Austretende Personen haben unterschriftlich zu bestätigen, dass alle schützenswerten Informationen (insbesondere besondere Personendaten), die ihnen zugänglich waren und die ausserhalb des Betriebes bearbeitet oder gespeichert wurden, unwiderruflich gelöscht (einfaches Löschen genügt nicht) oder zurückgegeben wurden.

## Passwörter

Passwörter sind vertraulich zu behandeln. Sie sind verschlüsselt oder sicher eingeschlossen zu verwahren und vor Unbefugten zu schützen. Anderen Personen (z.B. Vorgesetzten, IT-Verantwortlichen, DSV, Familienmitgliedern usw.) sind Passwörter unter keinen Umständen bekannt zu gegeben.

Grundsätzlich müssen Passwörter mindestens zwölf Stellen lang sein und sollen eine Kombination von Klein- und Grossbuchstaben, Ziffern und Sonderzeichen enthalten. Leicht zu erratende Passwörter und solche, die einen Bezug zur eigenen Person aufwei-

sen (z.B. Name, Name von Angehörigen, Geburtsdatum usw.), sind nicht erlaubt. Geschäftlich genutzte Passwörter dürfen nicht privat verwendet werden. Sie sind sofort zu ändern, wenn ein Verdacht besteht, dass sie Dritten bekannt geworden sind. Ein früher bereits benutztes Passwort darf nicht mehr gewählt werden.

Für Aufnahme- und Messgeräte mit einem Passwortschutz sowie für das lokale Login an Arbeitsstationen, welche ein starkes Passwort bereits für das Entschlüsseln zum Hochfahren des Gerätes benötigen, ist ein einfacheres Passwort zulässig.

Gruppenpasswörter werden nur vergeben, wenn dies zwingend erforderlich ist. Sie sind umgehend zu ändern, wenn sich die Zusammensetzung der Gruppe verändert. Gleiches gilt für alle Passwörter, wenn sie unautorisierten Personen bekannt geworden sind. Initialpasswörter müssen sofort geändert werden.

## Datensicherung, -löschung und Entsorgung von Informationsträgern

Geschäftsbezogene Daten müssen auf zentralen Datenspeichern des Betriebes gespeichert werden. Die / der DSV sorgt für eine regelmässige Sicherung aller Geschäftsdaten.

Nicht mehr benötigte Daten müssen von Datenträgern (z.B. USB-Datenträger, Speicherkarten usw.) unwiederbringlich gelöscht werden (einfaches Löschen genügt nicht). Nicht mehr benötigte Informationsträger (z.B. USB-Datenträger, CD-ROM usw.), die vertrauliche Informationen enthalten oder einmal enthielten, sind physikalisch zu vernichten (z.B. Schreddern).

## Firewall und Malware-Schutz

Die Mitarbeitenden dürfen die Sicherheitssoftware (Malwareschutz, Firewall usw.) nicht ausschalten, blockieren oder ihre Konfiguration verändern. E-Mails mit unbekanntem Absender, verdächtigem Betreff oder unüblichem Inhalt sind sehr vorsichtig zu behandeln, da sie von der Schutzsoftware nicht erkannte Malware enthalten könnten. Ihre Anhänge sowie Links auf Websites sollen keinesfalls geöffnet werden. Jeder Verdacht auf Malware muss sofort der / dem DSV gemeldet werden.

## Hard- und Software

Die Mitarbeitenden dürfen keine Software und keine Hardware-Erweiterungen, insbesondere keine Kommunikationseinrichtungen und externe Massenspeicher installieren bzw. anschliessen, ausser sie wurden im Einzelfall dazu berechtigt. Die Mitarbeitenden dürfen Informatiksysteme, die am Netzwerk angeschlossen sind, nicht gleichzeitig mit einem Netz oder System ausserhalb des internen Netzwerks verbinden.

Nur für die ICT verantwortliche Personen dürfen Geräte in die Reparatur oder zur Entsorgung geben. Sie stellen sicher, dass keine schützenswerten Daten auf diesem Weg den Betrieb verlassen.

Änderungen an den Systemeinstellungen (Installation, Deinstallation, Änderung der Konfiguration usw.) dürfen nur durch  für die ICT verantwortliche Personen oder im Auftrag dieser vorgenommen werden.

# Nutzung von Kommunikations- und Internetdiensten

## Allgemein

Allgemein gilt für die Kommunikation, unabhängig ob über Internet, Telefon oder vor Ort, dass vertrauliche Informationen nur mitgeteilt werden dürfen, wenn sichergestellt ist, dass keine unberechtigte Dritte (dazu zählen z.B. auch Mitarbeitende mit einer anderen Berechtigung, Familienmitglieder beim Home Office, Teilnehmende ohne ein Recht an dieser Information an Sitzungen und Dritte in der Nähe der Besprechung usw.) diese Information damit auch bekanntgemacht wird. Dabei sind auch geöffnete Fenster oder Türen zu beachten.

Internetdienste, wie fremde Email-Domains (bluewin, gmx, gmail usw.), Online-Dateiablagen, Online-Kalender oder oder nicht auf den Betrieb lautende Messenger-Dienste, dürfen nicht für geschäftliche Zwecke verwendet werden.

## Email unter der Domain [betrieb.ch]

E-Mails mit vertraulichem Inhalt (zum Beispiel besonders schützenswerte Personendaten oder Passwörter zur Entschlüsselung oder einen Download) müssen verschlüsselt versandt werden. Es reicht, wenn der sensible Inhalt in eine verschlüsselte Datei gepackt (ZIP), als Anhang einer normalen Email angehängt wird. Zur Übermittlung von Passwörter zur Entschlüsselung oder einem Download-Zugang an Berechtigte eignet sich auch der SMS-Dienst oder die Bekanntgabe am Telefon oder an einer Sitzung (ohne dass dies Unberechtigte auch bekannt gemacht wird).

Das automatische Weiterleiten von E-Mails und das Freigeben der persönlichen Mailbox an eine Drittperson sind nicht erlaubt. Bei mehrtägigen Abwesenheiten ist die Funktion des Abwesenheitsassistenten zu nutzen.

Das E-Mail-System darf in zurückhaltendem Mass auch für private Zwecke verwendet werden. Das Versenden von E-Mails mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt, mit unnötig grossem Verteiler oder mit der Aufforderung zum Weiterversand im Schneeballsystem ist verboten. Private E-Mails müssen entweder umgehend gelöscht oder in einem persönlichen Ordner mit der Bezeichnung «privat» abgelegt werden.

## Internetseiten, Interrnetplattformen und Clouds

Der Zugriff auf Websites mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt und der zu privaten Zwecken erfolgende Zugriff auf Chatprogramme, Tauschbörsen und Online-Ticker sind verboten. Das Herunterladen und Installieren von Software aus dem Internet ist grundsätzlich nicht gestattet. Das vom System angeforderte herunterladen und installieren von Updates für das OS oder zu bereits installierten Apps ist jedoch Pflicht. Auch der/die DSV kann das Herunterladen oder die Installation solcher Dateien erlauben.

Geschäftsrelevante Daten dürfen nur mit dem formellen Einverständnis der [Geschäftsführung] im Internet publiziert werden.

Schützenswerte Informationen und grosse Mengen nicht anonymisierter Personendaten dürfen nur verschlüsselt (zum Beispiel mit https) über das Internet übermittelt werden.

[Variante 1: Die private Nutzung sozialer Netzwerke (Facebook, LinkedIn, TikTok, X usw.) soll möglichst ausserhalb der Arbeitszeit erfolgen. Während der Arbeitszeit ist sie auf ein Minimum zu beschränken].

[Variante 2: Die private Nutzung sozialer Netzwerke (Facebook, LinkedIn, TikTok, X usw.) ist nicht erlaubt.]

Eine Bekanntgabe Informationen die den Betrieb betreffen in sozialen Netzwerken (Facebook, LinkedIn, TikTok, X usw.) ist nur nach Genehmigung durch die [Geschäftsleitung] zulässig, die Bekanntgabe von Personendaten verboten.

### Collaborations und Besprechungs Tools und

Werden Mitarbeitende eingeladen an einer Videokonferenz teilzunehmen oder Arbeitsdaten über ein Collaboration Tool zu teilen, bestimmt in der Regel die einladende Person das Produkt eines Anbieter (einige Anbieter stellen diesbezüglich unterschiedliche Produkte zur Verfügung, welche sich oft bezüglich dem Datenschutz unterscheiden). Bestimmen Mitarbeitende das Tool, haben sie das von der/vom DSV empfohlene Tool den Teilnehmenden vorzuschlagen und als Alternative die von der/vom DSV freigegebenen Tools anzubieten.

Vertrauliche Informationen dürfen nur bei der Verwendung eines durch die/den DSV dazu freigegeben Tool bekannt gemacht werden.

### Virtual Private Network (VPN)

Eine VPN-Verbindung zwischen einer Arbeitsstation und dem zentralen Datenspeicher des Betriebes, ist sicherheitstechnisch einer Verbindung über das Netzwerk des Betriebs gleichgestellt.

## Private Nutzung betrieblicher, betriebliche Nutzung privater ICT

Die zurückhaltende Benützung von IT-Mitteln für private Zwecke ist grundsätzlich gestattet, soweit dadurch die Systemressourcen wie Speicher und Übertragungskapazität nicht im Übermass belastet werden. Die private Nutzung soll möglichst ausserhalb der Arbeitszeit erfolgen. Während der Arbeitszeit ist sie auf ein Minimum zu beschränken. Private Daten müssen lokal in einem persönlichen Verzeichnis mit der Bezeichnung «privat» oder auf dem persönlichen Netzwerklaufwerk «[PFAD]:\» gespeichert werden.

Geschäftsdaten dürfen grundsätzlich nicht privat genutzt oder in privaten Geräten oder Medien gespeichert werden. Private Geräte dürfen nur mit Bewilligung der/des DSV für bestimmte geschäftliche Aufgaben eingesetzt oder mit dem betrieblichen Netzwerk verbunden werden.

## Einsatz mobiler Geräte

Beim Einsatz mobiler Geräte sind folgende Punkte zu beachten:

- Auf mobilen Geräten (zum Beispiel Notebooks, USB-Datenträger, Smartphones) müssen Dokumente mit vertraulichem beziehungsweise schützenswertem Inhalt verschlüsselt gespeichert werden.
- Mobile Arbeitsgeräte müssen verschlüsselt sein, so dass diese nur mit einem Boot-Passwort gestartet werden können.
- [Variante 1: Die Benutzerinnen und Benutzer von mobilen Arbeitsstationen sind selbst für die Datensicherung und die datenschutzgerechte Aufbewahrung verantwortlich.]
  [Variante 2: Die Benutzerinnen und Benutzer von mobilen Arbeitsstationen legen geschäftliche Arbeitsdaten in einem lokalen Arbeits-Verzeichnis ab, welches bei einer Verbindung des Geräts mit dem Netzwerk des Betriebes, mit dem entsprechenden Verzeichnis in der zentralen Datenspeicherung synchronisiert wird.]
  Die Berechtung für den Zugriff auf lokale Daten, darf dem in der zentralen Datenhaltung nicht widersprechen.
- Mobile Geräte, welche Personendaten oder sonstige vertrauliche Daten enthalten dürfen in öffentlich zugänglichen Räumen nicht unbeaufsichtigt gelassen werden.
- Die Geräte dürfen nicht Dritten zur Nutzung überlassen werden.
- Der Verlust eines mobilen Gerätes ist unverzüglich der / dem DSV zu melden.
- Es dürfen keine zusätzlichen Apps installiert werden. Besteht ein begründeter Bedarf, ist die Genehmigung der respektive des IT-Verantwortlichen einzuholen.
- Eine Verbindung zu drahtlosen Netzwerken (zum Beispiel WLAN) ist nur zulässig, wenn eine verschlüsselte Übertragung eingesetzt wird.
- Drahtlose Schnittstellen (Bluetooth, WLAN, NFC) sind bei Nichtgebrauch zu deaktivieren.
- Die Ortungsdienste sind bei Nichtgebrauch zu deaktivieren.

## Ausnahmen

Die / der DSV entscheidet über Ausnahmen von der vorliegenden Weisung. Entsprechende Gesuche sind ihr / ihm mit Begründung per E-Mail einzureichen.

## Protokollierung und Kontrolle

Zur Überwachung des richtigen Funktionierens, der Sicherheit, der Integrität und der Verfügbarkeit der Informatik werden Systeme eingesetzt, die Protokolle und Warnmeldungen erzeugen. Internetzugriffe werden aufgezeichnet und ein halbes Jahr gespeichert. Eine personenbezogene Auswertung ist nur nach vorgängiger Information der davon betroffen Mitarbeitenden möglich.

Ein grob fahrlässiges, widerrechtliches oder weisungswidriges Verhalten im Umgang mit Datenschutz und Informationssicherheit kann straf-, zivil- und/oder arbeitsrechtliche Konsequenzen haben.