DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Checkliste für Benutzungsreglemente betreffend mobile Geräte

1. Zweck und Zielgruppe

Die gegenständliche Checkliste dient der Hilfestellung für die Prüfung und Erstellung von Reglementen über die Benutzung und Handhabung von mobilen Endgeräten. Sie hilft dabei insbesondere, bestehende **Reglemente auf inhaltliche Vollständigkeit zu überprüfen**. Zu diesem Zweck wird nachstehend in den Abschnitten 2 bis 5 der Mindestinhalt eines Benutzungsreglements aufgeführt.

Die Checkliste richtet sich speziell an Verantwortliche im Bereich der Informationstechnologie, die Benutzungsreglemente oder Dienstvorschriften für die Nutzung von mobilen Arbeitsplätzen (z. B. Notebooks, Tablets oder Smartphones) erstellen.

2. Information und Hinweise

Ein Reglement für die Nutzung mobiler Endgeräte sollte zumindest Folgendes beinhalten:

2.1. **Versionsmanagement:** Die Versionsnummer und das Datum des Dokuments, das Datum des Inkrafttretens und bei allenfalls befristeten Reglementen das Datum des Ausserkrafttretens. ☐

2.2. **Dokumentenlenkung:** Kommunikation, wo die jeweils gültige Version abrufbar ist. ☐

2.3. **Sachlicher Geltungsbereich**: Bezeichnung der vom Reglement betroffenen Hardwarekategorien; Abgrenzung zur Telearbeit oder Einbezug derselben. ☐

Beispiele: Mobile Arbeitsplätze und Datenträger im Allgemeinen wie insbesondere Notebooks, Smartphones aber auch USB-Speichersticks, optische Datenträger usw.

2.4. **Persönlicher Geltungsbereich**: Bezeichnung des vom Reglement betroffenen Personenkreises. ☐

Beispiele: Angestellte einer Gemeindeverwaltung, Aussendienstmitarbeiter usw.

2.5. **Begriffsdefinitionen**: Definition der wichtigsten im Reglement verwendeten Begrifflichkeiten, wobei insbesondere technische Begriffe erläutert werden sollten. ☐

Beispiel: Unter mobilen Geräten versteht man einerseits Endgeräte, die aufgrund ihrer Grösse und ihres Gewichts ohne grössere körperliche Anstrengung tragbar, vom Stromnetz unabhängig und somit mobil einsetzbar sind. Andererseits sind auch mobile Datenträger mobile Geräte.

2.6. **Verweis auf Dokumentation** sowie allfällige weitere Handbücher für den sicheren und datenschutzkonformen Umgang mit dem jeweiligen mobilen Gerät. ☐

2.7. **Hinweis** auf Art und Umfang **allfälliger Massnahmen zur Überwachung der Umsetzung** der Regeln des Reglements. ☐

Beispiele für Überwachungsmassnahmen: Protokollierung der Verwendung von USB-Anschlüssen an Arbeitsstationen, Detektion von Softwareinstallationen.

2.8. **Hinweis** auf die **verpflichtende Natur** des Reglements sowie auf **allfällige Sanktionskataloge.** ☐

3. Allgemeine Regelungen

Ein Reglement für die Nutzung mobiler Endgeräte sollte zumindest folgende Punkte regeln:

3.1. **Informationen und personenbezogene Daten** die mobil verarbeitet werden dürfen ☐

Beispiel: Die Verarbeitung von als vertraulich klassifizierten Dokumenten ist auf mobilen Geräten nicht zulässig.

3.2. **Mitnahme** mobiler Geräte ☐

Beispiele: Verbot der Mitnahme mobiler Geräte in bestimmte Länder; Notebooks dürfen das Betriebsgelände nicht verlassen; nur wer von der Geschäftsleitung dazu autorisiert wurde, darf Notebooks ins Ausland mitnehmen.

3.3. **Private Nutzung betrieblicher** mobiler Geräte ☐

Beispiele: Die Synchronisierung von E-Mails, Kontakten oder Kalender mit einem privaten Rechner ist nicht zulässig; Verbot geschäftliche Geräte an Bekannte auszuleihen; für private Termine ist ein eigener Kalender zu verwenden.

3.4. **Betriebliche Nutzung privater** mobiler Geräte ☐

Beispiele: Privates Notebook in Schulungs- oder Präsentationsräumen, privates Mobiltelefon für geschäftliche Kommunikation; Bedingungen für die Installation von Software zur Synchronisation von privaten mobilen Geräten auf den geschäftlichen Arbeitsplätzen.

Im Zusammenhang mit **Bring Your Own Device** (BYOD) sind jedenfalls spezifische Regelungen zu treffen. Beispielsweise die strikte Einhaltung der Trennung zwischen geschäftlichen und privaten Daten, verbindliche Verhaltenspflichten (vgl. dazu Pkt.3.8, 3.10 und 3.11), die Fernlöschung bei Verlust, die Installation von Drittanbietersoftware, die Vorgehensweise bei Beendigung des Arbeitsverhältnisses usw. Das Umgehen der Sicherheitsarchitektur des Betriebssystems bspw. mittels Jailbreak oder das Rooten ist nicht gestattet.

3.5. Datenverarbeitung auf „**Poolgeräten**“ (Leihgeräte zur vorübergehenden Nutzung) ☐

Beispiel: Der Benutzerspeicher von Poolgeräten muss bei der Rückgabe vollständig und sicher gelöscht werden.

3.6. **Administration** und **Verwaltung** der mobilen Geräte ☐

Beispiele: Die Informatikdienste haben exklusiven Zugriff auf die Sicherheitseinstellungen; welcher Mitarbeiter wann welche (Pool-)Geräte ausser Haus einsetzt wird protokolliert; die Installation oder Nutzung nicht genehmigter Software bzw. bei Smartphones sogenannter Apps ist nicht zulässig; der Einsatz einer Mobile Device Management Lösung ist vorgeschrieben.

3.7. **Datensicherung/Datensynchronisation** bei der mobilen Nutzung ☐

Beispiele: Berichtigungs- und Löschbegehren betroffener Personen müssen bei Synchronisation und Sicherung der Daten des mobilen Geräts berücksichtigt werden; das Gerät ist in regelmässigen Abständen zu synchronisieren.

3.8. Nutzung sogenannter **Cloud-Dienste** (Outsourcing) ☐

Beispiel: Nutzung von nicht autorisierten/öffentlichen Cloud-Diensten zur mobilen Datenverarbeitung (bspw. zur Datensicherung) ist nicht zulässig.

3.9. Verwendung mobiler **Datenträger an Arbeitsplätzen** ☐

Beispiele: USB-Ports werden blockiert und allfällige DVD-Laufwerke sind deaktiviert.

3.10. **Sicherung** mobiler Geräte **gegen Diebstahl** ☐

Beispiele: Mobile Geräte dürfen beim Transport und beim Einsatz ausserhalb der Räumlichkeiten des Arbeitgebers (etwa im Rahmen von Konferenzen, in Hotelzimmern usw.) nicht unbeaufsichtigt gelassen werden; Mobile Geräte dürfen nicht in Fahrzeugen zurück gelassen werden oder dürfen zumindest nicht von aussen sichtbar sein.

3.11. Vorgehen bei **Verlust oder Diebstahl** mobiler Geräte ☐

Beispiele: Jeder Mitarbeitende muss die Kontaktdaten der bei Verlust zu benachrichtigenden Stelle bei sich führen; Geräte, die abhandenkommen und wieder gefunden werden, dürfen erst nach Zurücksetzen auf Werkseinstellungen oder vollständiger sicherer Löschung wieder verwendet werden.

3.12. **Entsorgung** von mobilen Datenträgern ☐

Beispiele: Vor Weitergabe vollständig und sicher löschen; bei der Entsorgung mechanisch zerstören.

3.13. Nutzung von sogenannten **ortsabhängigen Diensten** *(engl. location based services)* sowie über die Auswertung und Verwendung möglicher protokollierter Bewegungsprofile ☐

Beispiel: Die Auswertung von Protokollen zur Überwachung der Mitarbeitenden findet nicht statt; wenn nicht notwendig, sind ortsabhängige Dienste zu deaktivieren.

4. Regelungen betreffend die lokale Verarbeitung und Datenträger

Zur lokalen Verarbeitung und Speicherung von personenbezogenen Daten auf mobilen Geräten sollte ein Reglement insbesondere regeln:

4.1. Massnahmen zur Sicherung der **Vertraulichkeit und Integrität** ☐

Beispiele: Verschlüsselung von USB-Sticks, HDs/SSDs oder sonstiger digitaler Speichermedien; geschäftliche Mobiltelefonie ist nur zulässig, wenn niemand das Gespräch mithören kann; mobil geführte Telefongespräche dürfen keinen vertraulichen Inhalt aufweisen; Notebooks, Telefone und Tablets müssen per PIN oder auf andere Weise vor unbefugtem Zugriff geschützt sowie mit einer automatischen Sperre nach einem bestimmten Zeitintervall abgesichert werden.

4.2. Massnahmen zur Sicherung der **Verfügbarkeit und Belastbarkeit** ☐

Beispiele: Vorgabe zur Häufigkeit von Backups; vorrätig halten von Ersatz-Akkus; Reparatur nur bei vertrauenswürdigen Fachbetrieben.

4.3. Massnahmen zur Sicherung gegen **unbefugte Benutzung** ☐

Beispiele: Mobile Geräte bei Nichtgebrauch unter Verschluss aufbewahren; kein Anbringen von Logos oder Klebern auf den Geräten; kein die Herkunft des Geräts bezeichnender Bildschirmschoner.

4.4. Verwahrung beim physischen **Transport** oder den **Postversand** von mobilen Datenträgern ☐

Beispiel: Nur verschlüsselte Datenträger dürfen mit der Post verschickt werden.

4.5. **Verwendung** von mobilen **Datenträgern** ☐

Beispiele: Die Verwendung von USB-Sticks ist nicht zulässig; es dürfen nur die USB-Sticks verwendet werden, welche vom Informatikdienst herausgegeben werden.

4.6. **Dokumentation der Weitergabe** von mobilen **Datenträgern** ☐

Beispiel: Die Heraus- oder Weitergabe von USB-Sticks muss quittiert werden; Notebooks müssen ein Lokalisierungssystem unterstützen.

5. Regelungen betreffend die Kommunikation

Im Zusammenhang mit der Datenkommunikation sollte ein Reglement insbesondere regeln:

5.1. Nutzung der **mobilen Telefonie** ☐

Beispiele: Erlaubnis privater Gespräche über mobile Geräte; Löschen von SMS und privaten Telefonnummern aus den verschiedenen Speichern und Listen vor der Rückgabe bspw. von Poolgeräten; Regeln zur Nutzung des Internets über mobile Datenverbindung (z. B. Roaming).

5.2. Nutzung von öffentlichen oder anderen **Zugängen ins Internet** ☐

Beispiele: Auf Konferenzen, in Sitzungszimmern und Schulungsräumen; die Nutzung von Public Access Points ist nur zulässig, wenn dabei Verschlüsselung eingesetzt wird; Einsatz von VPN Software.

5.3. Nutzung von **Drahtlos-Schnittstellen** wie WLAN oder Bluetooth ☐

Beispiel: Firewall gegen Zugriffe auf das mobile Gerät; Bluetooth darf nicht verwendet werden; Schnittstellen dürfen lediglich kurzzeitig und nur bei Bedarf eingeschaltet werden.

Diese Checkliste ist eine Hilfestellung aus Datenschutzsicht für die Prüfung und Erstellung von Reglementen über die Benutzung und Handhabung von mobilen Endgeräten. Sie erhebt *keinen* Anspruch auf Vollständigkeit und darf deshalb nicht als ein rechtlich verbindliches Dokument betrachtet werden.