5/2019
97 – 120

Kurzmeldung
Body-Cams & Polizei
Viktoria Haidinger

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Auskunft

ISSN 2313-5409

dako.manz.at

MANZ

Österreichische Post AG PZ 18Z041356 P Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

Mag. Ing. Markus Oman, CSE/Mag. jur. Siegfried Gruber
Geschäftsführender Gesellschafter O.P.P. – Beratungsgruppe/Prokurist O.P.P. – Beratungsgruppe

Checkliste

Checkliste IKT-Nutzungsrichtlinie inkl Zusatzdokumente

Diese Checkliste zeigt die Struktur einer IKT-Richtlinie und einer eventuell notwendigen Betriebsvereinbarung.

Erforderliche Dokumente bei Unternehmen mit Betriebsrat

IKT-Nutzungsrichtlinie als Dienstanweisung bedingt folgende Dokument

- zwingende Betriebsvereinbarung nach § 96 Abs 1 Z 3 ArbVG über Kontrollmaßnahmen, die die Menschenwürde berühren, und
- Kenntnisnahme jedes einzelnen Mitarbeiters durch Unterschrift direkt am Dokument (kann Verpflichtung nach § 6 DSG und Zustimmung zur Verwendung des eigenen Bildes enthalten) oder
- schriftliche Kenntnisnahme zB auf einer Liste (ev auch elektronisch geführt) unter Verweis auf die aktuelle Version der RL durch jeden einzelnen Mitarbeiter (kann Verpflichtung nach § 6 DSG und Zustimmung zur Verwendung des eigenen Bildes enthalten).

IKT-Nutzungsrichtlinie als freiwillige Betriebsvereinbarung nach § 97 Abs 1 Z 1 ArbVG (Hinweis: jede Änderung ist nur mit Zustimmung des Betriebsrats möglich) bedingt folgende Dokumente:

- IKT-Nutzungsrichtlinie inkl entsprechender Kontrollmaßnahmen als Betriebsvereinbarung und
- schriftliche Verpflichtung jedes einzelnen Mitarbeiters nach § 6 DSG und Zustimmung zur Verwendung des eigenen Bildes.

Erforderliche Dokumente bei Unternehmen ohne Betriebsrat

IKT-Nutzungsrichtlinie als Dienstanweisung bedingt folgende Dokumente:

- Kenntnisnahme und Zustimmung zu den Kontrollmaßnahmen gem § 10 AVRAG jedes einzelnen Mitarbeiters durch Unterschrift direkt am Dokument (kann Verpflichtung nach § 6 DSG und Zustimmung zur Verwendung des eigenen Bildes enthalten) oder
- schriftliche Kenntnisnahme zB auf einer Liste (ev auch elektronisch geführt) unter Verweis auf die aktuelle Version der RL und Zustimmung zu den Kontrollmaßnahmen gem § 10 AVRAG durch jeden einzelnen Mitarbeiter (kann Verpflichtung nach § 6 DSG und Zustimmung zur Verwendung des eigenen Bildes enthalten).

IKT-Nutzungsrichtline

Einleitung

- Geltungsbereich und Inkrafttreten
- Zielsetzung
- Organisation und Ansprechpartner

Arbeitsplatzcomputer und Netzwerk

- Allgemeines
  - Generelle Bestimmungen zur Ausgestaltung des Arbeitsplatzes und deren Beschaffung, insb Regelungen zum empfohlenen Verbot der Verwendung firmenfremder Hardware (bring-your-own-device).
- Zugriffsschutz
  - Regelungen zur Verwendung von Benutzerdaten (Benutzername/Passwort), allenfalls 2-Faktor-Authentifizierung, sowie Regelungen zur Komplexität (zB mindestens 8-stellig, Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen) und Gültigkeitsdauer von Benutzerkennungen.
- Zugriff auf das Firmen-Netzwerk
  - Regelt die Bedingungen, unter denen Berechtigungen zum Zugriff auf das Firmennetzwerk und darauf gespeicherte Daten erteilt (zB nach genehmigten Antrag durch den Vorgesetzten) und entzogen werden.
- Zugriff zu Anwendungen
  - Die Berechtigung des Zugriffs zu Anwendungen sollte ausschließlich nach dem „need to know" Prinzip erfolgen. Dies gilt für Benutzer, aber auch für Administratoren.
- Virenschutz
  - Die Verwendung eines jeweils aktuellen Virenschutzes ist verpflichtend vorzusehen (in der Regel durch automatisches Update). Ein Deaktivieren des Virenschutzes ist nicht zulässig.
- Physische Sicherheit

Mobile Endgeräte

- Daten auf mobilen Endgeräten
  - Der Zugriff auf Daten auf mobilen Endgeräten bedarf eines besonderen Schutzes.
- Einbindung in fremde Netzwerke
  - Fremde Netze (zB Kunden-Netze, WLAN-Hotspots) weisen oft im Vergleich zum eigenen Firmennetzwerk stark reduzierte Sicherheitsmaßnahmen auf. Die Nutzung öffentlicher Netze sollte nur unter Umsetzung zusätzlicher Sicherheitsmaßnahmen (zB zwingende Nutzung einer Firmen-VPN-Verbindung, Nutzung von mobilen Netzwerken des Telekommunikations-Anbieters des Unternehmens) erlaubt sein.
- Diebstahlschutz
  - Regelungen zur sicheren Aufbewahrung von mobilen Endgeräten im Hotel bzw PKW; Anzeigepflicht bei Verlust.

Remote-Zugänge/Telearbeit

- Soweit Fernzugriffe auf das Firmennetzwerk über Remote-Verbindungen zugelassen sind, sollten (über die rein arbeitsrechtlichen Fragen hinaus) insb Regelungen zur rechtmäßigen Nutzung von Endgeräten und der Zugriff auf Daten des Unternehmens geregelt sein (keine Mitnutzung von Familienmitgliedern). Insb ist der Schutz unberechtigter Kenntnisnahme durch Dritte (zB anhand von Ausdrucken) zu gewährleisten.

Betriebliche Software

- Installation von privater Software
  - Neben allfälligen urheberrechtlichen Problemen ergibt sich durch den Einsatz privater Software auch die Gefahr, dass Schadprogramme „eingeschleust" werden. Soweit möglich empfiehlt sich das Verbot der Installation privater Software.

Daten

- Datentypen
  - Durch die Definition von Datentypen (anhand von Risikokategorien – zB öffentlich/intern/geheim) und Zuweisung dieser Datentypen zu Verarbeitungsvorgängen können jeweils dem Risiko angemessene Datensicherheitsmaßnahmen ergriffen werden. Die Datentypen und die damit in Zusammenhang mit stehenden (va organisatorischen) Datensicherheitsmaßahmen sollten den Mitarbeitern bekannt sein.
- Datenschutz, Datengeheimnis und Datenweitergabe
  - Ausführungen dazu, was iZm der Verarbeitung personenbezogener Daten iS des Datengeheimnisses gem § 6 DSG zu beachten ist. Insb sollte beschrieben werden, welche Verarbeitungen und Weitergaben von personenbezogenen Daten (pbD) zulässig sind, bzw was explizit nicht erlaubt ist.

Datenspeicherung und -sicherung

- Datenträger
  - Soweit pbD auf Datenträgern gespeichert werden, die nicht (bzw nicht mehr) mit Endgeräten verbunden sind, ist zu beschreiben, wie diese Daten zu schützen sind (zB Verwendung verschlüsselter USB-Sticks), bzw wie diese Datenträger einer Entsorgung zuzuführen sind.
- Ausgedruckte Daten
  - Zum Schutz pbD vor unbefugter Kenntnisnahme sind auch Ausdrucke entsprechend den Regelungen hinsichtlich „Datentypen" (siehe oben) zu schützen; zB durch Umsetzung einer Clear-Desk-Policy (siehe *Pollirer,* Was versteht man unter den Begriffen Clear Desk/Clear Screen-Policy? Dako 2019/21) bzw der Nutzung von Aktenvernichtern anstatt von Papierkörben.

Internet, E-Mail & Telefonie

- Internet
  - Insb Regelungen iZm der privaten Nutzung.
- Internet Download/Upload
  - Beschreibung von erwünschtem bzw verbotenem Verhalten. Soweit möglich sollte dies durch technische Einstellungen erzwungen werden (Black-Lists).
- E-Mails
  - Neben den allgemeinen Regelungen zur Nutzung (Netiquette) sollten insb auch die Zulässigkeit privater Nutzung sowie idZ anzuwendende Regeln beschrieben werden.
- Webmail
  - Soweit ein Zugriff auf den E-Mail-Account über öffentliche Internet-Dienste zulässig ist, sollten die idZ zwingend einzuhaltenden Sicherheitsmaßnahmen beschrieben werden (siehe oben „Remote Zugänge", „Einbindung in fremde Netze", „mobile Endgeräte").
- Datensicherheit der E-Mail-Kommunikation (beachte branchenspezifische Normen)
- Posteingang – Empfangen von Attachments
- Postausgang – Senden von Attachments
- Fehlerhafte E-Mails
  - Was passiert mit E-Mails, wenn der Name des Empfänger falsch oder unvollständig ist (Empfehlung für EDV-Abteilungen: keine automatische Antwort, allenfalls Weiterleitung an den vermuteten Empfänger durch den Administrator).
- E-Mail-Konten ausgeschiedener Mitarbeiter
  - Soweit private Nutzung zugelassen war, eine Regelung zur Herausgabe und anschließenden Löschung privater E-Mails. Regelungen über automatisierte Antwort bzw Weiterleitung an Stellvertreter.
- Verhaltensweisen für die E-Mail-Nutzung
  - Siehe oben unter E-Mails: Netiquette, Verwendung von Abwesenheits-Nachrichten, E-Mail-Signatur.
- Telefonie
- Smartphones
  - Insb Regelungen über die Privatnutzung, aber auch Regelungen über die Installation von (allenfalls kostenpflichtigen) Apps.
- MDM – Mobile Device Management
  - Anweisungen zur erwünschten Vorgehensweise iZm dem Verlust eines mobilen Endgeräts (zur Gewährleistung einer Ortung bzw Remote-Löschung von Daten).

Protokollierung
- Kontrollmaßnahmen
  - Beschreibung zulässiger bzw unzulässiger Kontrollmaßnahmen. Kontrollmaßnahmen müssen zur Erreichung des Kontrollzweckes grundsätzlich geeignet und wirksam sein.
- Betriebe mit Betriebsrat
  - Betriebsvereinbarung zwingend erforderlich.
- Betriebe ohne Betriebsrat
  - Einwilligung eines jeden Mitarbeiters erforderlich.

Rückgabe von Firmeneigentum
- Telefon
- Token/Key
- Laptop/Tablet
- USB Datenträger
- Papiervordrucke/Visitkarten

Sanktionen – Was passiert bei Zuwiderhandlung?
Schlussbestimmungen
Kenntnisnahme durch MA

Eckpunkte einer Betriebsvereinbarung über die Verwendung personenbezogener Daten von AN und Kontrollmaßnahmen iZm der Nutzung von IT-Systemen
Gegenstand und Geltungsbereich
- Was regelt diese BV?
- Für wen gilt diese BV?
- Geschlechterbezeichnung

Zielsetzung der Betriebsvereinbarung sind
- Qualitätskriterien
- Persönlichkeitsrechte/Datenmissbrauch
- Gefahren der Überwachung

Datenverwendung
- Zweck
- Gesetzliche Verpflichtungen
- Weitergaben
- Autorisierungen

Mitwirkungsrechte des Betriebsrats
- Wann ist der BR einzubinden?
- Rechte des BR

Protokollierung
- Arten von Protokolldaten (allgemeine/Nachweis rechtmäßige Verwendung)
- Aufbewahrungsfristen der Protokolldaten

Kontrollmaßnahmen
- Auswertung Protokolldaten iZm Verwendung personenbezogener Daten
- Auswertung gesetzliche/arbeitsvertragliche Protokolldaten
- Auswertung bei Missbrauch
- Organisatorische Belange der Auswertung
- Unzulässige Auswertungen

Gültigkeit der Betriebsvereinbarung
- Start
- Dauer
- Bedingungen oder Änderung

Dako 2019/59