ABl 12/2025, S. 304-307

Richtlinie zum Umgang mit personenbezogenen und betrieblichen Daten am Arbeitsplatz (Clean-Desk-Policy)

Präambel

In den Organisationseinheiten des Bischöflichen Ordinariates werden aufgrund der Dienstvereinbarung Telearbeit (Home-Office) sowie künftig mit Inkrafttreten der Dienstvereinbarung mobiles Arbeiten vermehrt Arbeitsplätze von den Mitarbeitenden zeitweise nicht genutzt. Auch für ungenutzte Arbeitsplätze fallen dabei Kosten für Raummiete, Heizung etc. an. Das Bistum ist bestrebt, wo immer möglich, Kosten der Verwaltung zu reduzieren. Sog. „Desk-Sharing“, also das Teilen eines Arbeitsplatzes mit wechselnden Kolleginnen und Kollegen, ist eine Maßnahme, um Raumkosten nachhaltig zu senken. In Organisationseinheiten, in denen „Desk-Sharing“ eingeführt wird, ist es erforderlich, dass die jeweils temporär zugewiesenen Arbeitsplätze am Ende eines Arbeitstages frei sind von Akten, Notizen, persönlichen Gegenständen etc., um denjenigen Kolleginnen und Kollegen, welche den Arbeitsplatz am kommenden Tag nutzen, ein störungsfreies Arbeiten zu ermöglichen.

Diese Richtlinie zum Umgang mit personenbezogenen und betrieblichen Daten am Arbeitsplatz ist ein Instrument, um sicherzustellen, dass alle sensiblen/vertraulichen Dokumente aus dem Arbeitsbereich eines Arbeitsplatznutzers entfernt und weggeschlossen werden, wenn sie nicht aktuell bearbeitet werden oder Mitarbeitende ihren Arbeitsplatz verlassen. Unberechtigte Personen (Besucherinnen und Besucher, auch Kolleginnen und Kollegen anderer Organisationseinheiten etc.) dürfen keinen Zugriff auf sensible/vertrauliche Dokumente erhalten.

Eine „Clean-Desk-Policy“ ist eine Strategie, um das Risiko von Sicherheitsverletzungen zu reduzieren. Sie soll auch das Bewusstsein aller Mitarbeitenden für den Schutz sensibler Informationen erhöhen.

1. Zweck

Zweck dieser Richtlinie ist es, die Mindestanforderungen für die Aufrechterhaltung eines „sauberen Schreibtisches und Desktops" festzulegen, um sensible/kritische Informationen über unsere Kolleginnen und Kollegen, unsere Betriebs- und Geschäftsgeheimnisse, unser geistiges Eigentum, die Kirchenmitglieder und unsere Lieferanten zu schützen. Eine „Clean-Desk-Policy“ zählt auch zu den standardmäßigen grundlegenden Datenschutzkontrollen.

2. Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeitenden der Organisationseinheiten des Bischöflichen Ordinariates, die am sog „Desk-Sharing“ teilnehmen. Sie gilt darüberhinaus für Mitarbeitende in Organisationseinheiten, in denen personenbezogene Daten oder Daten, die dem Betriebs- und Geschäftsgeheimnis unterliegen, verarbeitet werden, unabhängig davon, ob sich die entsprechenden Arbeitsplätze in Einzel- oder Mehrplatzbüros, in der betrieblichen Arbeitsstätte oder am heimischen Arbeitsplatz bzw. bei mobilem Arbeiten an unterschiedlichen Arbeitsorten befinden.

3. Grundsätzliche Anforderungen

- Bei Verlassen des Arbeitsplatzes müssen alle Akten, Ausdrucke, Kopien oder dergleichen so verstaut werden, dass diese Dokumente für unbefugte Dritte unzugänglich sind (beispielsweise durch Abschließen des Einzelbüros oder des

Schreibtisches, Schließfach, absperrbare Rollcontainer, abschließbare Spinde, Datenträgersafe o. ä.).

- Lassen Sie keine Ausdrucke im Drucker/Kopierer liegen. Nutzen Sie z. B. die Möglichkeit der PIN-Identifikation beim Multifunktionsdrucker.
- Bewahren Sie Passwortnotizen an einem sicheren und unzugänglichen Ort auf.
- Der Bildschirm des Rechners am Arbeitsplatz muss in Pausen, auch bei nur kurzfristigem Verlassen des Arbeitsplatzes, gesperrt werden. Passwörter müssen der Passwortrichtlinie entsprechend. Geben Sie niemals ihr Passwort weiter. Unbeaufsichtigte, nicht gesperrte Computer sind ein hohes Sicherheitsrisiko. Unbefugte könnten so Zugang zu vertraulichen Daten erhalten.
- Lassen Sie nicht zu, dass Außenstehende Ihnen über die Schulter schauen, wenn Sie vertrauliche Daten auf dem Monitor haben. Zusehen bei der Eingabe von Passwörtern ist grundsätzlich auszuschließen – auch unter Kolleginnen und Kollegen.
- Stellen Sie ihren Bildschirm so ein, dass Besucher oder andere Unbefugte ihn nicht einsehen können, bei mobilem Arbeiten ist immer eine Sichtschutzfolie für den Bildschirm zu verwenden. Achten Sie auch darauf, ob ein Ausspähen ggf. unbemerkt über ein Fenster oder eine Türe geschehen könnte. Führen Sie Telefonate mit Bedacht. Schließen Sie die Türe ihres Büros oder gehen Sie ggf. in einen separaten Raum bzw. eine Kommunikationsbox. Wo dies alles nicht möglich ist, versuchen Sie möglichst keinen Personenbezug am Telefon preiszugeben.
- Der tägliche Datenmüll enthält oft sensible Personendaten oder Daten des Betriebs- und Geschäftsgeheimnisses und darf nach Arbeitsende nicht unverschlossen, z. B. in einem Papierkorb unter dem Bürotisch, liegen bleiben. Entsorgen Sie Ihren Datenmüll in den dafür vorgesehenen Datentonnen oder Aktenvernichtern.

4. Arbeitsplatzausstattung

Es gilt die Richtlinie für die Ausstattung von Büroarbeitsplätzen bei „Desk-Sharing“, im Besonderen:

- verbleiben Bürostühle am Arbeitsplatz – keine Zuweisung „privater Bürostühle“,
- können keine privaten Gegenstände (Bilder, Dekorationen, Topfpflanzen oder Sonstiges) am „Desk-Sharing-Arbeitsplatz“ zugelassen werden. Diese gehören in den Rollcontainer, persönlichen Spind o. ä.,
- verbleiben keine Tisch-/Schreibunterlagen auf dem Schreibtisch. Diese sind bei Arbeitsende im Rollcontainer, persönlichen Spind o. ä. aufzubewahren,
- ist der Schreibtisch am Arbeitsende von Schmutz und Rändern (Kaffeetasse etc.) zu säubern,
- wird der Schreibtisch sowie Armstützen am Bürostuhl vom jeweiligen Arbeitsplatznutzenden bei Arbeitsende desinfiziert,
- ziehen Laptop, Tastatur, Kopfhörer und Maus (wie auch Locher, Tacker, Stifte etc.) mit dem Arbeitsplatzwechsel um und bleiben nicht am Arbeitsplatz. Sie sind im Rollcontainer, persönlichen Spind o. ä. aufzubewahren,
- ist es für Mitarbeiterinnen und Mitarbeiter mit Funktastatur und -maus ratsam, den USB-Empfänger unmittelbar am Laptop anzuschließen statt an der Dockingstation. Dies ermöglicht eine bessere Verbindung zwischen den Geräten und beugt Verlusten vor.

5. Einhaltung der Richtlinie

5.1 Messung der Einhaltung

Das Datenschutzteam sowie die interne Revision und die jeweiligen Dienstvorgesetzten sind befugt, die Einhaltung dieser Richtlinie durch ihre jeweiligen Methoden zu überprüfen, einschließlich, aber nicht beschränkt, durch regelmäßige Begehungen, Berichte, interne und externe Audits und Bericht an die jeweilige Hauptabteilungsleitung oder an den Generalvikar.

5.2 Ausnahmen

Jede Ausnahme von der Richtlinie muss im Voraus vom Dienstvorgesetzten in Abstimmung mit dem Informationssicherheits- bzw. Datenschutzbeauftragten genehmigt werden. Ausnahmegenehmigungen bedürfen der Schrift-, wenigstens der Textform.

5.3 Zuwiderhandlungen

Zuwiderhandlungen gegen diese Richtlinie stellen eine Verletzung der arbeitsvertraglichen (Neben-)Pflichten dar und können entsprechende arbeitsrechtliche Konsequenzen nach sich ziehen.

6. Inkrafttreten

Diese Richtlinie tritt zum 1. Juni 2025 in Kraft. Alle dieser Richtlinie entgegenstehenden Regelungen werden hiermit aufgehoben.