FAQ: Datenschutz im Berufsalltag

Es gibt kaum noch Bereiche, in denen personenbezogene Daten nicht regelmäßig verarbeitet werden. Ein bedachter und verantwortungsvoller Umgang hilft, die Gefahr von Datenpannen auf ein Minimum zu reduzieren. Im Folgenden finden Sie einige Anregungen für einen datenschutzkonformen Umgang, welche an dieser Stelle unter Berücksichtigung der häufigsten Datenpannen am Arbeitsplatz zusammengefasst wurden.

Sichern Sie Ihren Arbeitsplatz vor Zugriffen Dritter

Beim Verlassen des Arbeitsplatzes dürfen keine Dokumente und Dateien mit personenbezogenen Daten offenliegend zurückgelassen werden. Sichern Sie aus diesem Grund die verwendeten Endgeräte per passwortgeschützten Sperrbildschirm, schließen Sie geöffnete Akten und verwahren Sie diese nach Möglichkeit in verschließbaren Aktenschränken. Bei einer längeren Abwesenheitszeit sind zudem die Büroräume zu verschließen. Dabei sollten die verwendeten Schlüssel keine näheren Bezeichnungen enthalten, die im Falle eines Verlustes Rückschlüsse auf die Zugehörigkeit zulassen. Geben Sie zudem unter keinen Umständen personengebundene Schlüssel oder Passwörter weiter.

Schützen Sie personenbezogene Daten vor neugierigen Blicken

Zum Schutz vor neugierigen Blicken sollte Ihr Arbeitsplatz so eingerichtet sein, dass Besucher oder andere unbefugte Dritte keine Einsicht auf Ihren Bildschirm nehmen können. Ist dies aufgrund der örtlichen Gegebenheiten nicht möglich, können Blickschutzfolien einen gleichwertigen Effekt erzielen. Die Verwendung von Blickschutzfolien empfiehlt sich außerdem bei der Nutzung mobiler Endgeräte an öffentlichen Plätzen und in Verkehrsmitteln. Besucher der Geschäftsräume sollten stets nur unter Aufsicht Zugang erhalten.

Geben Sie keine Auskünfte an unbefugte Dritte

Generell gilt bei der Erteilung von Auskünften, dass sowohl das berechtigte Interesse des Auskunftssuchenden als auch das schutzwürdige Interesse der betroffenen Person zu beachten und gegeneinander abzuwägen sind. Sofern eine Auskunft telefonisch verlangt wird, besteht die größte Schwierigkeit darin, den Anrufer eindeutig zu identifizieren. Vereinbaren Sie hierbei gegebenenfalls einen Rückruf und überprüfen Sie die hierfür angegebene Telefonnummer mit möglicherweise bereits bekannten Nummern.

Ansonsten gilt: Prüfen Sie die Befugnis des Anfragenden, eine derartige Auskunft zu erhalten. Dieser muss sein Auskunftsrecht nachweisen, auch wenn es sich um Polizei oder Staatsanwaltschaft handelt. Beschränken Sie die Auskunft auf den absolut notwendigen Umfang und erteilen Sie die Auskünfte in Textform.

Nutzen Sie E-Mail- und Internetdienste bewusst

Achten Sie bei der Verwendung von Internet und E-Mail auf verdächtige oder ungewöhnliche Inhalte. Öffnen Sie Anhänge oder Links in E-Mails nur dann, wenn Sie den Absender kennen und einen Phishing-Versuch sicher ausschließen können. Weitere Informationen hierzu erhalten Sie auch auf unserem Merkblatt „Umgang mit Phishing-E-Mails“.

Trennen Sie Berufliches von Privatem

Die Trennung von beruflichen und privaten Angelegenheiten ist auch im Bereich des Datenschutzes unbedingt zu beherzigen. Dementsprechend sollten über den vom Arbeitgeber zur Verfügung gestellten Arbeitsmitteln, wie beispielsweise Endgeräte und Zugänge zu E-Mail-Postfächern, ausschließlich für geschäftliche Zwecke genutzt werden. Ebenso ist der Einsatz von privaten Geräten und Zugängen für geschäftliche Zwecke zu unterlassen, sofern dies nicht ausdrücklich von der Geschäftsführung erlaubt wurde.

Vernichten Sie Dokumente und Hardware mit personenbezogenen Daten datenschutzgerecht

Werden Dokumente oder Hardware mit personenbezogenen Daten nicht mehr benötigt, sind diese datenschutzkonform zu entsorgen. Dabei muss sichergestellt werden, dass die Möglichkeit eines weiteren Zugriffs oder einer Wiederherstellung ausgeschlossen werden kann. Eine einfache Entsorgung der jeweiligen Datenträger über den Hausmüll ist nicht ausreichend. Papierunterlagen sind zumindest zu schreddern (vgl. DIN 66399, DIN EN 15713), Festplatten fachgerecht, beispielsweise über einen speziellen Dienstleister, zu entsorgen. Beachten Sie zudem, dass moderne Multifunktionsgeräte zum Teil ebenso über Festplatten verfügen, die personenbezogene Daten enthalten können.

Achten Sie auch im Homeoffice auf einen datenschutzkonformen Umgang

Auch bei der Arbeit im Homeoffice muss auf einen datenschutzkonformen Umgang mit personenbezogenen Daten geachtet werden. Stellen Sie aus diesem Grund sicher, dass Sie sämtliche der hier aufgeführten Anregungen stets auch bei der Arbeit zu Hause umsetzen.

Meldung von Datenschutzverletzungen

Sollte Ihnen dennoch eine Datenschutzverletzung unterlaufen sein oder haben Sie Kenntnis von einer solchen erlangt, wenden Sie sich bitte umgehend sowohl an Ihren Vorgesetzten als auch an Ihren Datenschutzbeauftragten. Diese untersuchen den Vorfall und entscheiden anschließend über das weitere Vorgehen.

Die häufigsten Datenschutzverletzungen am Arbeitsplatz

1. Dokumente mit personenbezogenen Daten landen im Papierkorb
2. Verwendung privater Geräte, wie z.B. USB-Sticks am Arbeitsplatz
3. Firmengeräte werden für private Zwecke genutzt
4. Nutzung des privaten E-Mail-Accounts für geschäftliche E-Mails
5. Triviale Passwörter
6. Offene Büros mit offenliegenden Dokumenten
7. Erteilung von zu weitreichenden Auskünften
8. Chaos am Arbeitsplatz
9. Fehlende Ordnerstrukturen
10. Verschweigen von Datenschutzverletzungen