



PRESSEMITTEILUNG

Berlin, 22. Oktober 2026

Höchststand bei Datenschutzvorfällen

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit verzeichnet einen Höchststand bei den gemeldeten Datenschutzvorfällen. Bereits in den ersten drei Quartalen 2026 erreichten die Behörde so viele Meldungen wie im gesamten Jahr 2025. Gründe dafür sind unter anderem schnellere und professionellere Cyberangriffe durch den Einsatz von KI.

Datenschutzvorfälle – umgangssprachlich auch Datenpannen genannt – sind Verletzungen des Schutzes personenbezogener Daten, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten führen. Von Januar bis einschließlich September 2026 erreichten die Berliner Datenschutzbeauftragte insgesamt 1.550 Meldungen solcher Vorfälle. Darunter entfallen 1.303 auf den nicht-öffentlichen Bereich und 247 auf den öffentlichen Bereich. „Das sind rund 40 Prozent mehr Meldungen von Datenschutzvorfällen als im gleichen Zeitraum 2025 bei meiner Behörde eingingen“, erklärt Meike Kamp, Berliner Beauftragte für Datenschutz und Informationsfreiheit.

Bei den Meldungen steigt zudem der Anteil von Datenschutzvorfällen aufgrund von Cyberangriffen. In Unternehmen und Behörden entstehen immer mehr digitale Angebote und Schnittstellen, durch die die Angreifer:innen in IT-Systeme gelangen können. KI in ihren Händen spielt dabei eine wesentliche Rolle: Sicherheitslücken können von Hacker:innen auch ohne Spezialkenntnisse leichter aufgespürt und ausgenutzt werden. Insbesondere lassen sich durch den Einsatz von KI professionell aussehende Phishing-Mails auch durch unspezialisierte Angreifer:innen leicht gestalten und ganze Kampagnen mit weniger Aufwand planen und durchführen. Außerdem lassen sich Cyberangriffe durch KI einfacher automatisieren und laufen deshalb sehr viel schneller ab.

Meike Kamp, Berliner Beauftragte für Datenschutz und Informationsfreiheit: „Mithilfe von KI können Hacker:innen Cyberangriffe schneller und professioneller durchführen. Dadurch fallen sie den

verantwortlichen Stellen später auf und sind häufiger erfolgreich. Umso wichtiger ist es daher, dass Verantwortliche kontinuierlich in die Sicherheit ihrer IT-Systeme investieren und sicherstellen, dass diese immer auf dem neuesten Stand sind. Verantwortliche sollten Zugriffsberechtigungen differenziert in ihrer Organisation erteilen, Notfallpläne vorbereiten und klare Zuständigkeiten zuweisen. Immer wieder erreichen uns Meldungen zu Vorfällen, bei denen personenbezogene Daten abgeflossen sind, die längst hätten gelöscht sein müssen. Doch auch das beste Löschkonzept hilft nicht, wenn nicht vorher erfasst wurde, wo überhaupt Daten anfallen und gespeichert werden. Verantwortliche müssen daher das Management personenbezogener Daten auf ihren Systemen umfassend beherrschen.“