Noch keine guten Vorsätze für das neue Jahr? (Hinweis auf Löschpflichten)

Sehr geehrte Datenschutz-Kunden,

wie in den Medien umfangreich berichtet wurde ist Ende des vergangenen Jahres das bisher höchste Bußgeld einer Datenschutzaufsichtsbehörde in Deutschland verhängt worden. Getroffen hat es die Wohnungsbau- und -verwaltungsgesellschaft Deutsche Wohnen SE in Berlin. Das verhängte Bußgeld beläuft sich auf 14,5 Mio. Euro. Was war passiert?

Die Deutsche Wohnen geriet bereits 2017 (also bevor die EU-DSGVO verbindliches Recht wurde) in das Visier der Datenschutzaufsichtsbehörde, die insbesondere die verwendete Archivierungssoftware und Archivierungspraktik bemängelt hat. Insbesondere die dauerhafte Speicherung von Daten, welche die Mietinteressenten (und damit teilweise die späteren Mieter) im Rahmen ihrer Mietbewerbung offenbart haben, wurden dauerhaft gespeichert. Hierzu gehören z. B. Einkommens- und Verdienstnachweise, Sozialversicherungsdaten, Kopien von Arbeitsverträgen etc.

Wir halten also fest: Die Daten wurden (zumindest zum weit überwiegenden Teil)
- rechtens erhoben (zur Anbahnung bzw. Durchführung eines Vertragsverhältnisses) und
- es handelt sich NICHT um die in Art. 9 EU-DSGVO benannten besonderen Arten personenbezogener Daten, bei denen ein erhöhtes Schutzbedürfnis unterstellt wird.

Obwohl sich die Deutsche Wohnen zur Mängelbeseitigung zur Zusammenarbeit mit der Aufsichtsbehörde bereit erklärt und erste konkrete Schritte eingeleitet hat, wurde dies zwar „mildernd“ berücksichtigt, die veranlassten Maßnahmen gingen nach Ansicht der Behörde aber nicht weit genug.

Bemängelt wurde, dass in der verwendeten Software eine rechtskonforme, also differenzierte Löschung von Daten, für die der Grund zur Verarbeitung weggefallen ist, nicht vorgesehen war und auch keine manuelle Löschung (oder Anonymisierung) stattgefunden hat. Klar, letzteres wäre bei ca. 165.000 Wohnungen im Bestand (Angabe entsprechend der Deutsche Wohnen SE) auch nicht ganz einfach gewesen. Damit wurden Datenbestände geführt, für die der Rechtsgrund der Verarbeitung entfallen ist, bei Mietern also z. B. Daten der Mietbewerbung, bei ehemaligen Mietern darüber hinaus auch Daten aus dem Mietverhältnis.

Konkret bezieht sich die Aufsichtsbehörde auf Verstöße gegen Artikel 5 (Grundsatz der Datenminimierung und Speicherbegrenzung) und Artikel 25 (Datenschutz durch Technikgestaltung) der EU-DSGVO. Auch Bestandsdaten müssen regelmäßig dahingehend einer Revision unterzogen werden, ob der Grund für ihre Verarbeitung noch gegeben ist.

Volker Baron (Dipl.-Geograph / IT-Systemelektroniker) – **Tel.:** +49 89 18923500 – **Fax:** +49 89 18923501
Büro: Haydnstraße 2, 80336 München – **E-Mail:** volker.baron@baron-consult.de – **Internet:** www.baron-consult.de
Finanzamt München I, USt-ID: DE 216791626
Bankverbindung: Münchner Bank eG, IBAN: DE84 7019 0000 0000 3389 15, BIC: GENODEF1M01

Für die Beurteilung der Rechtmäßigkeit kommt ggf. auch in Betracht, dass der ursprüngliche Grund für die Verarbeitung vielleicht entfallen ist, aber eine neue Rechtsgrundlage herangezogen werden kann. Daten, die ursprünglich zur Anbahnung und Durchführung des Mietverhältnisses verarbeitet wurden, sind nach Kündigung des Mietverhältnisses ggf. auf Basis einer gesetzlichen Verpflichtung vorzuhalten – in aller Regel aber nicht alle Daten, sondern eben nur die rechtlich geforderten. Auch nach Ablauf gesetzlicher Speicherfristen kann sich der Grund für die Verarbeitung wandeln. Befindet sich der Verantwortliche in einem länger andauernden Rechtsstreit mit dem Betroffenen, kann ggf. auf das berechtigte Interesse an der Speicherung der Daten verwiesen werden, z. B. wenn es sich um für den Rechtsstreit erhebliche Sachverhalte handelt, die der Verantwortliche zur Nachweisführung benötigt.

Geht man nunmehr noch davon aus, dass es neben den „Kunden“ branchenabhängig noch weitere Betroffenengruppen gibt (eigene Mitarbeiter, Bewerber, Lieferanten, bei sozialen Einrichtungen z. B. Betreute und ehrenamtliche Helfer, bei Vereinen z. B. Mitglieder etc.), dann wird deutlich, dass es sich um ein sehr komplexes Thema handelt. Und natürlich gibt es auch eine Norm zum Thema: DIN 66398 „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“. Weil ich die Sache für meine Kunden aber nicht kompliziert, sondern umsetzbar machen möchte, hier meine Handlungsempfehlungen:

1. Schritt: Sie ermitteln alle Betroffenengruppen und die von ihnen gespeicherten Datenkategorien. Diesen Schritt haben wir schon ein gutes Stück erledigt, wenn unser Verzeichnis von Verarbeitungstätigkeiten vollständig und aktuell ist.

2. Schritt: Sie definieren die Löschfristen für die einzelnen Datenkategorien. Hierbei sind mindestens solche Datenkategorien zu differenzieren, bei denen unterschiedliche Rechtsgründe und / oder unterschiedliche Aufbewahrungsfristen in Betracht kommen. Hinterfragen Sie bitte, ob Sie den spontan gewählten Rechtsgrund (also z. B. eine erteilte Einwilligung oder Ihr berechtigtes Interesse an der Verarbeitung) auch bei einer verschärften Nachfrage nachweisen bzw. vertreten können. Vergessen Sie nicht, den Startzeitpunkt der Aufbewahrungsfrist festzulegen, also z. B. „Zeitpunkt der Erhebung der Daten“ / „Ende des Vorgangs“ / „Zeitpunkt der Beendigung der Geschäftsbeziehung“. Orientieren Sie sich hierbei an der Formel „Frist + Startzeitpunkt + Datenkategorie = Löschregel“).

3. Schritt: Entwerfen Sie aus den unter 1. und 2. gewonnen Erkenntnissen ein Lösch- und Archivierungskonzept, in dem mindestens folgende Punkte benannt sind:

- Wie identifiziere ich zu löschende Daten? Werde ich hierbei durch die eingesetzten Softwareprodukte unterstützt? Müssen bereits bei der Erfassung der Daten Eintragungen vorgenommen werden, die eine spätere Identifikation der zu löschenden Daten ermöglichen (z. B. bei Notizen zu Anfragen, die nicht zu einem Vertragsabschluss geführt haben).
- Wie führe ich eine vollständige Löschung der Daten durch, für deren Verarbeitung der Rechtsgrund entfallen ist? Welche Funktionen müssen ausgelöst werden? Wo muss manuell eingegriffen werden, z. B. durch manuelles Löschen oder durch Anonymisierung (Überschreiben von Name, Anschrift und Geburtsdatum des Betroffenen)?
- Wer ist für die Durchführung verantwortlich?
- Wie werden die Löschläufe dokumentiert / protokolliert?

Wenn Sie also noch keine „guten Vorsätze“ für das neue Jahr gefasst haben und Sie aus meinen Ausführungen Defizite in Ihrem Datenschutzmanagement erkennen konnten: Wie wäre es, sich dieses Jahr dem Thema „Löschung nicht mehr benötigter Daten“ zu widmen?

In jedem Fall wünsche ich Ihnen, dass Sie sich möglichst viele Ihrer Wünsche erfüllen können und Sie von guter und stabiler Gesundheit durch das Jahr begleitet werden.

München, 2020-01-07

Volker Baron

PS: Wer sich über meine Ausführungen hinaus mit der DIN 66398 auseinandersetzen möchte, aber den vom Beuth-Verlag angesagten Preis 125,00 € scheut, kann sich eine Vorversion der Norm kostenlos herunterladen:
https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKE-wie9NPyjvLmAhVEzKQKHSVoCx4QFjAAegQIBRAC&url=https%3A%2F%2Fwww.secorvo.de%2Fpublikationen%2Fdin-leitlinie-loeschkonzept-hammer-schuler-2012.pdf&usg=AOvVaw3LNBZuugJaRu86WbTbXwGU

(Hinweis: Externe Verlinkungen meiner Datenschutz-Newsletter stehen zu einem späteren Zeitpunkt gegebenenfalls nicht mehr zur Verfügung)