Die Landesbeauftragte für den Datenschutz Schleswig-Holstein

ULD: 40. Tätigkeitsbericht 2021

Die Landesbeauftragte für Datenschutz Schleswig-Holstein, hat am 22. Februar 2022 ihren Tätigkeitsbericht für das Jahr 2021 vorgelegt. Der Bericht greift zahlreiche Themen des Datenschutzes und der Informationsfreiheit auf, mit denen sich das Unabhängige Landeszentrum für Datenschutz (ULD) im vergangenen Jahr beschäftigt hat. Wiederkehrende Probleme: Missbrauch vorhandener Daten, Rechtsverstöße aus Unachtsamkeit und viele Datenpannen.

„Wie schon im Vorjahr war unsere Tätigkeit in 2021 von der Pandemie geprägt: Corona und Datenschutz, Corona und Informationsfreiheit – aber wir bekamen auch wieder Anfragen und Beschwerden zu einer breiten Palette von Themen, die alle möglichen Formen der Verarbeitung von Daten betrafen." Das ULD erhielt 1.464 Beschwerden zu mutmaßlichen Datenschutzverstößen, weitere 712 Beratungsanfragen wurden bearbeitet. Dies entspricht etwa den Zahlen des Jahres 2020. Eine Zunahme um 50 % war im Bereich der Informationsfreiheit zu verzeichnen, in dem das ULD in 78 Fällen eingeschaltet wurde – und häufig erreichen konnte, dass mehr Informationen herausgeben wurden. Hansen sieht dies als Ansporn zur Verbesserung der Situation im Land, denn: „Auch nach 22 Jahren Informationsfreiheit in Schleswig-Holstein läuft noch nicht alles rund. Die Nachvollziehbarkeit des Behördenhandelns hat aber gerade in Pandemie-Zeiten an Wichtigkeit gewonnen."

In einem anderen Bereich sieht man ebenfalls einen auffälligen Zuwachs, wie Hansen berichtet: „Im Vergleich zum Vorjahr stieg die Zahl der Datenpannen-Meldungen um etwa 60 %. Dennoch zeigt sich in unseren Prüfungen, dass es noch immer Fälle gibt, in denen die Verantwortlichen ihrer Meldepflicht nicht nachgekommen sind." Die Meldepflicht bei Verletzungen des Schutzes personenbezogener Daten – kurz: Datenpannen – ist eine rechtliche Anforderung und muss von den Verantwortlichen umgesetzt werden. Im Tätigkeitsbericht der Landesbeauftragten für Datenschutz finden sich viele Beispiele für Datenpannen. Hansen dazu: „Unser Bericht dient auch dazu, dass alle aus Fehlern lernen können, die passiert sind. Diese Beispiele können dabei helfen, das Risiko zu bewerten, das mit der Verarbeitung personenbezogener Daten in der eigenen Firma oder Behörde verbunden ist, und geeignete Gegenmaßnahmen zu treffen."

Selbst das simple Beispiel der QR-Codes verdeutlicht das Problem des Verstehens, denn Menschen können nicht direkt ersehen, welche Daten darin enthalten sind, sondern müssen das Muster erst per Smartphone scannen. Und: Wer bei einer Einlasskontrolle einen solchen QR-Code etwa als Impfnachweis vorzeigt, weiß nicht, ob dieser beim Scannen lediglich gelesen und die Gültigkeit geprüft wird oder ob der Code kopiert und die ausgelesenen Informationen gespeichert werden.

Einige der eingetretenen Datenpannen bezogen sich auf Verarbeitungen rund um das Impfen oder Testen. Andere hingen mit dem Arbeiten im Homeoffice zusammen, z. B. die Fälle, in denen Akten oder Datenträger auf dem Transport zwischen Dienstort und dem Zuhause abhandenkamen. Offene E-Mail-Verteiler, Fehladressierungen oder verlorene unverschlüsselte USB-Sticks gehören zu den Dauerthemen bei den Datenpannen-Meldungen. Der große Anstieg der Meldezahlen ergab sich aber aus mehreren Wellen von Angriffen über das Internet auf Server von Firmen und Behörden, bei denen personenbezogene Daten betroffen waren.

Hansen kommentiert dies: „Mit Sorge blicke ich auf das Thema Informationssicherheit. Einerseits haben immer noch viele Organisationen ihre Hausaufgaben nicht gemacht, um bekannte Schwachstellen in IT-Systemen zu beseitigen – die Datenpannen-Meldungen zeigen uns, wie solche Sicherheitslücken immer wieder ausgenutzt werden und oft auch Daten abfließen können. Andererseits mehren sich auch die Angriffe auf IT-Systeme, die nicht mit Updates in den Griff zu bekommen sind. Einige Akteure haben ein Interesse daran, Sicherheitslücken zu kultivieren statt sie zu schließen – dies ermöglicht dann ein heimliches Infiltrieren von Smartphones und Ausspionieren von Menschen mit Überwachungssoftware wie ‚Pegasus', die in vielen Ländern zum Einsatz kommt." Die Landesbeauftragte für Datenschutz sieht darin einen Verstoß gegen das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Hansen fordert: „Datenschutz und Sicherheit müssen eine Selbstverständlichkeit bei jeder Verarbeitung personenbezogener Daten sein."

Für die Verantwortlichen bedeutet dies, dass ihre eigenen Prozesse datenschutzgerecht zu gestalten sind. Bei der Auswahl von Produkten und Dienstleistern müssen sie sorgfältig vorgehen und Datenschutzkonformität einfordern. Wichtige Ansprechpartner sind die Datenschutzbeauftragten im Unternehmen oder in der Behörde.

Das bewusst missbräuchliche Verwenden von personenbezogenen Daten und das absichtliche Verstoßen gegen das Recht durch Verantwortliche und deren Dienstleister werden in der täglichen Arbeit des ULD, dessen Zuständigkeitsbereich auf Schleswig-Holstein beschränkt ist, vergleichsweise selten festgestellt. Sehr viel häufiger sind solche Fälle, in den die Verantwortlichen unachtsam waren oder die Datenschutzanforderungen grob fahrlässig ignoriert haben. Zu den am meisten nachgefragten Bereichen gehört die Videoüberwachung (179 Beschwerden, 36 Beratungsanfragen). Auch Datenschutz-Fehler bei der Website-Gestaltung – etwa durch ein unzulässiges Einbinden problematischer Tracking-Technik – sind mittlerweile stärker in den Fokus gelangt, beispielsweise im Rahmen der länderübergreifenden Branchenprüfung im Bereich Medien. Die rechtlichen Anforderungen und Hinweise zur korrekten Umsetzung lassen sich den Orientierungshilfen, Leitlinien und Informationsbroschüren entnehmen, die auf den Webseiten der Aufsichtsbehörden abrufbar sind.

Der Tätigkeitsbericht steht hier zum Download zur Verügung: *https://www.datenschutzzentrum.de/tb/tb40/*

Marit Hansen, Landesbeauftragte für Datenschutz Schleswig-Holstein