IT-Sicherheitstipp Nr.6 – August 2019

Umgang mit sensiblen Daten

Vertrauliche Daten

Wann sind Daten vertraulich? Grundsätzlich dann, wenn ihre Veröffentlichung oder ein unberechtigter Zugang schutzwürdige Interessen verletzen würden. Beispielhaft sei der Eintrag im standesamtlichen Geburtenregister, dass ein Kind adoptiert ist, genannt.

Die meisten von uns haben täglich mit Daten zu tun, die mehr oder weniger vertrauliche Inhalte haben. Oft fehlt das Bewusstsein, wie schnell vertrauliche Informationen in unbefugte Hände geraten können. Auslöser sind neben nicht vollständiger Kenntnis der rechtlichen Rahmenbedingungen (z.B. die jeweiligen Datenschutz- und ggf. Informationsfreiheitsgesetze) oft die fehlende Sensibilität im Umgang mit vertraulichen Informationen.

Der Schaden durch unsachgemäßen Umgang mit vertraulichen Daten kann beträchtlich sein und in vielen Fällen auch rechtliche Konsequenzen für den Verursacher bzw. die Verursacherin haben. Diese können arbeitsrechtliche bzw. disziplinarische, aber auch straf- und zivilrechtliche Folgen umfassen. Gegebenenfalls wird auch Schadensersatz gefordert.

Elektronische Datenverarbeitung

Schneller und direkter Zugriff auf Daten

Mit der zunehmenden Digitalisierung von Daten werden wichtige und kritische Informationen elektronisch verfügbar. Dadurch können sie schneller verarbeitet, aber auch unkontrolliert weitergeleitet und kopiert werden.

Dabei kann heute fast jede interne Information zum Nachteil Ihrer Verwaltung oder der Kundinnen und Kunden ausgenutzt werden. Wie alle wichtigen Daten müssen deshalb auch digitale Informationen vor unberechtigtem Zugriff geschützt werden. Das Datenschutzrecht und die Informationssicherheit verpflichten daher die Verwaltungen, technische und organisatorische Schutzmaßnahmen zu treffen.

Bevor Sie sensible Daten weitergeben, sollten Sie kurz drei Schritte prüfen:

1. Besteht eine Rechtsgrundlage zur Weitergabe personenbezogener Daten?
Zur Weitergabe personenbezogener Daten ist eine Rechtsgrundlage oder die Einwilligung der betroffenen Person erforderlich.

2. Kann ich der empfangenen Seite vertrauen? Darf sie die enthaltenen Informationen sehen?
Stellen Sie sicher, dass Sie die richtigen Adressaten verwenden. Weisen Sie gegebenenfalls darauf hin, dass die Daten vertraulich sind oder nicht weitergegeben werden dürfen.

3. Wohin gelangen die Informationen?
Insbesondere beim unverschlüsselten Versand über das Internet sollten Sie sicher sein, dass die Daten nicht vertraulich sind. Aber auch beim Senden an Drucker, die nicht an Ihrem Arbeitsplatz stehen, müssen Sie sicherstellen, dass keine Einsichtnahme durch Unbefugte möglich ist.

Weiterleitung von Informationen

Unter Umständen ist vor der Weitergabe das Einholen von Vertraulichkeitsverpflichtungen bzw. die Einwilligung der betroffenen Personen notwendig. Bei unverschlüsseltem E-Mail-Verkehr dürfen Sie nie vertrauliche Daten versenden. E-Mails sind wie Postkarten lesbar! Versenden Sie im Zweifelsfall Briefe.

Cybersicherheit

Wie erkenne ich vertrauliche Daten?

Sind die Daten durch gesetzliche oder behördliche Bestimmungen geschützt?

Die Verwaltungen unterliegen stets dem jeweils für sie gültigen Datenschutzgesetz. In einigen Ländern und beim Bund gibt es zudem Informationsfreiheitsgesetze, in denen u.a. ein Anspruch für jedermann auf Offenlegung der bei der Verwaltung vorliegenden Daten geregelt ist. Ausgenommen sind regelmäßig personenbezogene Daten und Betriebs- oder Geschäftsgeheimnisse. Hierdurch wird das Datenschutzrecht in den Bereich des Informationsfreiheitsrechts einbezogen.

Aber auch behördeninterne Regelungen, z.B. Verschlusssachenanweisungen, sind zu beachten.

Schutz von Betriebs- und Dienstgeheimnissen

Vertraulich? Intern? Geheim?

Zunächst gilt es, die Regelungen des Datenschutzrechts und ggf. des Informationsfreiheitsrechts zu beachten.

Besonders schutzbedürftig sind alle **personenbezogenen Daten**. Darunter versteht man „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“ (Art. 4 Abs. 1 EU-Datenschutzgrundverordnung). Hierzu zählen neben Name, Geburtsdatum und Anschrift auch das Kfz-Kennzeichen, Gesundheitsdaten und persönliche Vorlieben.

Darüber hinaus ist es denkbar, Daten in **Vertraulichkeitsklassen** einzustufen. Die Zuordnung zu einer bestimmten Klasse kann dann zu bestimmten Verhaltensregeln führen. Die folgenden Beispiele sollen zeigen, wie eine solche Zuordnung und die mit ihr verbundenen Regeln aussehen könnten. Sollte es keine behördlichen Regelungen in Ihrer Verwaltung zum Datenschutz geben, können diese Beispiele zur Orientierung dienen. Auch **Betriebs- und Geschäftsgeheimnisse** sind geschützt – selbst wenn ein Informationsfreiheitsgesetz Auskunftsansprüche gegenüber der Verwaltung schafft.

Nach den Informationsfreiheits- bzw. Transparenzgesetzen (zum Frühjahr 2018 jeweils für den Bund und alle Länder mit Ausnahme von Bayern, Hessen, Niedersachsen und Sachsen), ist ein Antrag auf Informationszugang zu einer Verwaltung abzulehnen, soweit durch die Übermittlung der Information ein Betriebs- oder Geschäftsgeheimnis offenbart wird und dadurch ein wirtschaftlicher Schaden entstehen würde.

Anders als zum Beispiel Informationen, die allgemein zugänglich sind und durch deren Verlust kein Schaden oder kein Verstoß gegen Auflagen (z.B. Prospekte, Broschüren, Webseite) entsteht, gibt es Daten und Informationen, deren Weitergabe Einschränkungen unterliegt.

Behördliche*r Datenschutzbeauftragte*r

Jede Behörde in der Europäischen Union ist nach dem Datenschutzrecht verpflichtet, eine*n Beauftragte*n für den Datenschutz zu benennen. Diese Person wacht über die Einhaltung der Datenschutzgesetze bei der Verarbeitung personenbezogener Daten. Sie ist zu besonderer Verschwiegenheit verpflichtet.

Der/die Datenschutzbeauftragte Ihrer Verwaltung kann Ihnen auch bei konkreten Fragen zum Datenschutz weiterhelfen.

Cybersicherheit

Kategorie 1: Interne Informationen

Natürlich sind auch **behördeninterne** Daten zu schützen!

Beispiele: Telefonlisten, Informationen über interne Arbeitsabläufe

Hinweise:

- Interne Informationen sind normalerweise nur für die Behördenbeschäftigten zugänglich. Sie dürfen nur mit Zustimmung der Leitungsebene nach außen gegeben werden.
- Vor der Weitergabe interner Informationen ist zu prüfen, ob eine Datenschutz- oder Vertraulichkeitserklärung abzuschließen ist.

Kategorie 2: Schützenswerte Informationen aus dem Behördenbereich

Beispiele: Personal- und Finanzdaten, Informationen über die Struktur der internen IT-Anlagen, entsprechend gekennzeichnete nichtöffentliche Verwaltungsunterlagen für die politischen Gremien und Niederschriften von nichtöffentlichen Sitzungen, Protokolle des Verwaltungsvorstandes

Hinweise:

- **Für wen?**
  Solche Informationen sollten nur dem Teil der Beschäftigten zur Verfügung gestellt werden, die diese für ihre Tätigkeit benötigt.
- **Bei Außenstehenden?**
  Bei Weitergabe an Dritte ist neben den Bedingungen, die für interne Informationen gelten, auch die Zustimmung der Leitungsebene erforderlich oder es gibt interne Regelungen.
- **Wie transportieren?**
  Es ist ein sicherer Transportweg zu wählen. Das heißt z.B. beim Versand über das Internet ist eine hinreichende Verschlüsselung zwingend notwendig.

Kategorie 3: Persönlich-vertrauliche Informationen

Persönlich-vertrauliche Informationen sind vor allem personenbezogene Daten nach dem Datenschutzrecht.

Beispiele: Personalakten, Daten der Gehaltsabrechnung, personenbezogene Daten von Bürgerinnen und Bürgern (z.B. Personenstand, Anträge).

Hinweise:

- Die Informationsfreiheitsgesetze schützen ausdrücklich personenbezogene Daten, auch wenn ein grundsätzlicher Auskunftsanspruch besteht.
- Unter bestimmten Voraussetzungen kann es aufgrund einer Einwilligung des Betroffenen zur Informationsmitteilung kommen.
- Prüfen Sie die Anforderungen genau! Eine einmal erteilte Auskunft kann nicht rückgängig gemacht werden!
- Persönlich-vertrauliche Informationen sollten besonders gekennzeichnet werden und dürfen von der empfangenden Stelle nur persönlich geöffnet werden.
- Sie sind für andere unzugänglich aufzubewahren.
- Eine Weitergabe oder sonstige Verarbeitung ist nur mit Einwilligung der betroffenen Person oder aufgrund gesetzlicher Bestimmungen zulässig.