Sensibilisieren, schulen und Verantwortung übernehmen

Datenschutz und IT-Sicherheit

Nach der Bundestagswahl 2021 besteht unter allen Parteien große Einigkeit: Die Digitalisierung des Landes muss endlich Fahrt aufnehmen. In den Kommunen werden schon heute immer mehr Daten digital verarbeitet. Dies können personenbezogene Daten wie Name und Anschrift sein, aber auch sensiblere Daten, wie Religionszugehörigkeit oder Gesundheitsdaten. Umso wichtiger ist es, dass dabei keine Datenlecks entstehen. Denn gerade in Deutschland sind Bürgerinnen und Bürger besonders sensibel, wenn es um den Schutz ihrer Daten geht.

Die DSGVO schafft Sicherheit und Vertrauen

Seit dem Jahr 2018 gilt in allen EU-Staaten die Datenschutz-Grundverordnung (DSGVO). Danach trägt die Leitung von Kommunen und kommunalen Betrieben eine besondere datenschutzrechtliche Verantwortung, sowohl für die rechtmäßige Verarbeitung von Bürgerdaten wie auch von Daten der eigenen Beschäftigten. Die konkrete datenschutzkonforme Gestaltung und Überwachung der Prozesse obliegt dann den Fachbereichsleitungen. Der betriebliche oder behördliche Datenschutzbeauftragte hat hierbei eine beratende und überwachende Funktion.

Eine Schlüsselrolle spielt die richtige Organisation von Verantwortlichkeiten und Vorgaben zum Datenschutz im eigenen Haus. Hierzu müssen alle datenschutzrelevanten Prozesse identifiziert und regelmäßig auf ihre rechtskonforme Durchführung überprüft werden. Werden die Informationspflichten eingehalten? Sind Ansprechpersonen und angegebene Verarbeitungszwecke noch aktuell? Und sind mit allen Auftragsverarbeitern die vorgeschriebenen Vereinbarungen getroffen worden?

All diese Informationen werden im Verarbeitungsverzeichnis zentral gesammelt, welches ebenfalls mindestens einmal jährlich durch die jeweiligen Fachbereiche auf seine Aktualität überprüft werden muss. Mit der Datenschutz-Grundverordnung sind auch Speicher- und Löschfristen erneut in den Fokus gerückt. Ein Löschkonzept sollte die Aufbewahrungsdauer aller erhobenen Daten festlegen und die für die Löschung verantwortliche Stelle benennen.

Und was, wenn es doch zu einer Datenschutzverletzung kommt? Dann ist das richtige Krisenmanagement gefragt. Da der Gesetzgeber strenge Fristen gesetzt hat, müssen Notfallpläne und Prüfschemata für den Fall des Falles bereits ausgearbeitet bereitliegen.

Beschäftigte sensibilisieren, um Datenpannen zu vermeiden

Damit die Notfallpläne möglichst nie gebraucht werden, müssen die Mitarbeitenden fortlaufend sensibilisiert werden – für den Datenschutz und für die Datensicherheit.

„Unter welcher Rechtgrundlage werden personenbezogene Daten erhoben, wie sehen die Informationspflichten aus und was muss ich beim Versand von personenbezogenen Daten via E-Mail beachten?“ Solche Fragen stellen sich Beschäftigte in Kommunen und kommunalen Betrieben häufig. In regelmäßigen Schulungen erfahren sie, wie sie mit diesen und weiteren Fragen umgehen müssen. Die Kommunal Agentur NRW hat mit Ko-Learning DATA ein passendes E-Learning-Angebot geschaffen. Wichtig ist, diese Schulungen zu dokumentieren, um sie im Fall einer Datenpanne gegenüber der Landesdatenschutzbeauftragten oder im Falle einer Klage auf Schadensersatz nachzuweisen. Bei Ko-Learning DATA erhalten alle Beschäftigten nach erfolgreichem Abschlusstest ein Zertifikat. Und die verantwortliche Person für den Datenschutz bekommt einen Überblick über die erfolgreiche Teilnahme an der Schulung.

Kein Bußgeld für öffentliche Stellen – Schadensersatzpflicht bleibt bestehen

Die Beauftragten für den Datenschutz und die Informationsfreiheit sind dafür zuständig, bei Verstößen ein Bußgeld zu verhängen. Allerdings greift hier die sog. Öffnungsklausel. Das Landesdatenschutzgesetz NRW nimmt somit in § 32 öffentliche Stellen von Geldbußen aus; es legt allerdings auch fest, dass dies nicht für Eigenbetriebe oder Anstalten des öffentlichen Rechts gilt, wenn diese personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten.

Was bei den möglicherweise sehr hohen Bußgeldern gegen Unternehmen in den Hintergrund getreten ist, sind die Schadensersatzansprüche nach Art. 81 Abs. 1 DSGVO, die eine geschädigte Person gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter geltend machen kann.
Voraussetzungen hierfür sind:

- Verstoß gegen Grundsätze zur Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 DSGVO
- entstandener materieller oder immaterieller Schaden
- schuldhafter, datenschutzrechtlicher Pflichtverstoß des Verantwortlichen oder Auftragsverarbeiters

Dabei sind auch öffentliche Stellen wie Kommunalverwaltungen oder Landesbehörden nicht von Schadensersatzforderungen ausgenommen. Hierbei ist auf den Schutz von Bürgerdaten sowie auf einen umfassenden organisatorischen Datenschutz zu achten, der auch Beschäftigten-, Bewerber- oder Dienstleisterdaten miteinbezieht.

Erste Urteile zum immateriellen Schadensersatz

In einer arbeitsrechtlichen Auseinandersetzung verurteilte das Arbeitsgericht Düsseldorf einen Arbeitgeber zu Schadensersatz, weil dieser dem Auskunftsanspruch des ehemaligen Arbeitnehmers nicht nachgekommen ist (ArbG Düsseldorf, Urteil vom 05.03.2020, 9 Ca 6557/18).

Das Arbeitsgericht Darmstadt sprach einem Bewerber Schadensersatz zu, weil das Unternehmen seine Gehaltsvorstellung an Dritte weitergab (LG Darmstadt, Urteil vom 26.05.2020, 13 O 244/19).

Das Arbeitsgericht Dresden verurteilte einen Arbeitgeber, der Gesundheitsdaten eines Arbeitsnehmers ohne ausreichende Rechtsgrundlage an eine Behörde weitergab (ArbG Dresden, Urteil vom 26.08.2020, 13 Ca 1046/20).

Neu ist das Konzept des Schadensersatzes im Datenschutz nicht. Schon nach § 7 BDSG (Bundesdatenschutzgesetz) konnte der Betroffene Schadensersatz geltend machen. Von dieser Regelung wurde allerdings nur selten Gebrauch gemacht.

Datenschutz ist nur so stark wie die IT-Sicherheit

Ein zweiter großer Faktor zur Vermeidung von Datenschutzpannen und Schadensersatzansprüchen ist die IT-Sicherheit. Hackerangriffe erreichen neue Höchststände. Ziele sind vermehrt öffentliche Stellen. Die Angreifer verschlüsseln die Daten auf den angegriffenen Rechnern und Servern mit sog. Ransomware und machen sie dadurch für deren Besitzer unbrauchbar. Mehrere Kommunen und kommunale Betriebe hatten deshalb in der Vergangenheit teilweise für Wochen keinen Zugriff auf ihre Systeme, IT-gestützte Aufgaben kamen fast zum Erliegen. Ein Zugriff ist häufig erst nach der Zahlung eines Lösegelds wieder möglich. Oft sind solche Angriffe auch gekoppelt mit dem Diebstahl großer Mengen an Daten, die unrechtmäßig weiterverkauft werden.

Die Täter setzen bei ihren Angriffen meist an der schwächsten Stelle der IT-Sicherheit an: den Mitarbeitenden. Sie werden zum Öffnen schädlicher E-Mail-Anhänge oder Links verleitet und gewähren den Hackern dadurch Zugriff auf das Behörden- oder Unternehmensnetzwerk. Auch hier ist eine regelmäßige Sensibilisierung der Beschäftigten wichtig, um ausgelegte Fallen zu umgehen. Neben grundsätzlichem Wissen zu Phishing, Social Engineering oder sicheren Passwörtern müssen klare Prozesse im Fall eines vermuteten oder tatsächlichen Angriffs festgelegt und bekannt sein.

Dabei ist die Devise: Lieber die E-Mail einmal mehr durch die IT-Abteilung auf Schadsoftware überprüfen lassen, als Hackern den Zugriff zu sensiblen Daten zu ermöglichen. Alle Beschäftig-

ten müssen somit in der Lage sein, mögliche Phishing-Mails zu erkennen und dem Verantwortlichen im Haus sofort zu melden, bevor innerhalb von Minuten ein teilweise irreversibler Schaden entstehen kann. Diese Themen wurden auch in der aktualisierten Version des Behörden-IT-Sicherheitstrainigs BITS angepasst, bspw. an die neuen Standards des Bundesamts für Sicherheit in der Informationstechnik. Ko-Learning BITS vermittelt in einem Online-Kurs Grundlagen der IT-Sicherheit. Auch hier wird der Kurs mit einem Abschlusszertifikat beendet.

Nicht zu unterschätzen ist bei allen Maßnahmen zur IT-Sicherheit eine umfassende Kommunikation der Gefahren, aber auch des Vorgehens der Kriminellen, um neue Tricks der Hacker abzuwenden. So müssen IT-Verantwortliche in immer kürzeren Abständen das Verhältnis von IT-technischen Einschränkungen und Arbeitserleichterungen durch zusätzliche technische Freiheiten abwägen. Eingeschränkte Voreinstellungen mindern dabei häufig den Arbeitskomfort und die Produktivität. Das führt häufig zu Frust bei Nutzern. Umso wichtiger ist es, dass IT-Verantwortliche stetig über die Gründe der Einschränkungen informieren und dies in möglichst verständlicher Sprache und mit der Möglichkeit, Rückfragen zu stellen.

Datenschutz und IT-Sicherheit müssen auch außerhalb des Büros gewährleistet sein

Nicht zuletzt aufgrund der zunehmenden Zahl an Heimarbeitsplätzen und des Arbeitens von unterwegs. Organisatorische Maßnahmen sind in beiden Fällen schwieriger einzuführen und zu überprüfen. Das fängt bei der Lagerung analoger Akten an und endet bei der Freigabe von Videokonferenzsystemen.

Mittlerweile haben viele Kommunen ihre Dienstanweisungen auf die neuen Arten des Arbeitens angepasst. Die Landesdatenschutzbeauftragten und das Bundesamt für Sicherheit in der Informationstechnik stellen praxisnahe Leitfäden bereit für das mobile Arbeiten und Entscheidungshilfen für die Beschaffung von Videokonferenzsystemen. Gerade bei Letzterem ist ebenso wie bei anderen cloudbasierten Diensten die Rechtsprechung des Europäischen Gerichtshofs zur Unwirksamkeit des Privacy Shields und somit der Übermittlung personenbezogener Daten in die USA (EuGH, 16.07.2020, C-311/18) zu beachten.

Unterstützung zu Datenschutz und Datensicherheit

Die zahlreichen Rechtsprechungen im Zusammenhang mit dem europäischen Datenschutzregime im Jahr 2020 machen deutlich: Auch zukünftig gibt es für die Kommunen organisatorischen Anpassungsbedarf zur Sicherstellung des datenschutzkonformen Arbeitens. Die Kommunal Agentur NRW unterstützt Sie gerne bei diesen Aufgaben.

Unsere Online-Schulungen

Mit Ko-Learning DATA schulen wir Beschäftigte u. a. zu den Themen:

- Grundbegriffe des Datenschutzes
- Bedingungen zur Verarbeitung von Daten
- Informationspflicht und Rechte betroffener Personen
- Datenschutz beim mobilen Arbeiten/Telearbeit
- Umgang mit Datenpannen

Mit dem Behörden-IT-Sicherheitstraining Ko-Learning BITS schulen wir Beschäftigte u. a. zu den Themen:

- Schadsoftware
- Cyberangriffe
- Umgang mit E-Mails
- Umgang mit Passwörtern

Ihr Ansprechpartner für Datenschutz:
Julian Salandi, Tel.: 0211 430 77 - 271,
E-Mail: salandi@KommunalAgentur.NRW

Ihr Ansprechpartner für IT-Sicherheit:
Karsten Klick, Tel.: 0211 430 77 - 107,
E-Mail: klick@KommunalAgentur.NRW