Die EU-Datenschutzgrundverordnung kommt

Am 25. Mai 2018 wird die europäische Datenschutzgrundverordnung verbindlich. Damit besteht erstmals in der Europäischen Union ein einheitliches Datenschutzrecht. Alle Länder der EU müssen ihre datenschutzrechtlichen Regelungen entsprechend anpassen. So erlässt NRW gerade ein Datenschutz-Anpassungs- und –Umsetzungsgesetz, das nach der 1. Lesung am 01.03.2018 derzeit in verschiedenen Fachausschüssen beraten wird.

Die neuen Regelungen sorgen für Unsicherheiten. Vielfach besteht die Besorgnis, plötzlich persönlich unüberschaubaren Risiken und hohen Bußgeldern ausgesetzt zu sein. Diese Sorge ist unbegründet: Die Vorschriften zu Sanktionen in der DSGVO erfassen nur Unternehmen. Die Regelung zur Ahndung von Verstößen gegen Datenschutzrecht durch Beschäftigte einer Einrichtung überlässt die DSGVO den Mitgliedstaaten. Nach unserer bisherigen Rechtslage (§ 34 unseres noch geltenden Datenschutzgesetzes NRW) begehen Beschäftigte eine Ordnungswidrigkeit, wenn sie vorsätzlich gegen datenschutzrechtliche Vorschriften verstoßen. Diese Regelung hat der Gesetzgeber nun nahezu wortgleich in den Entwurf des neuen Datenschutz-Anpassungs- und Umsetzungsgesetzes NRW übernommen. Es bleibt also dabei, dass die Gefahr, mit einem Bußgeld belangt zu werden, nur bei bewussten und gewollten Verstößen besteht.

Es wird sich auch nicht alles unter der neuen DS-GVO ändern. Die Verordnung enthält aber einige Änderungen, die Handlungsbedarf auslösen:

Nachweispflicht

Weitgehend unverändert schreibt die neue Datenschutzgrundverordnung die Grundsätze der Rechtmäßigkeit und Transparenz, Zweckbindung, Datenminimierung, sachlichen Richtigkeit und Aktualität fest.

Neu ist aber die Pflicht, auch nachweisen zu können, dass diese Grundsätze eingehalten werden. Ein solcher Nachweis erfordert eine umfassende Dokumentation der mit einer Datenverarbeitung verbundenen Risiken, der getroffenen technischen und organisatorischen Maßnahmen und auch eine Beschreibung, wie die Einhaltung der Datenschutzprinzipien durch die Beschäftigten sichergestellt wird (z.B. Dokumentation von Schulungsmaßnahmen, Rundschreiben, Checklisten).

Die DSGVO verlangt nicht nur, Maßnahmen einmalig festzulegen und zu implementieren, sondern auch ihre Wirksamkeit regelmäßig zu überprüfen und fortlaufend zu aktualisieren.

Verarbeitungsverzeichnis

Das bisherige Verfahrensverzeichnis wird nun durch ein sogenanntes Verarbeitungsverzeichnis abgelöst. Dabei müssen sowohl die verantwortlichen

Stellen als auch IT.NRW als Auftragsdatenverarbeiter ein Verzeichnis erstellen. Die jeweiligen Inhalte ähneln dem bisherigen Verfahrensverzeichnis, gehen aber auch darüber hinaus. Insofern müssen nicht nur für zukünftige Verfahren neue Verarbeitungsverzeichnisse erstellt werden. Vielmehr müssen die bestehenden Verfahrensverzeichnisse umgeschrieben werden und zusätzliche neue Verzeichnisse zu den Verfahren erstellt werden, bei denen IT.NRW Auftragsverarbeiter ist.

Muster für die Erstellung sind auf der Internetseite der LDI NRW unter https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Hinweis-und-Muster-zum-neuen-Verzeichnis-von-Verarbeitungstaetigkeiten/Hinweis-und-Muster-zum-neuen-Verzeichnis-von-Verarbeitungstaetigkeiten.html zu finden.

Datenschutz-Folgeabschätzung

Weiter wird die bisherige Vorabkontrolle durch eine Datenschutz-Folgeabschätzung abgelöst. Die Zuständigkeit hierfür liegt nunmehr unmittelbar beim Fachbereich. Inhalte sind die Beschreibung und Bewertung der Verarbeitungsvorgänge, der datenschutzrechtlichen Anforderungen, der Risiken für die Rechte der betroffenen Personen und der geplanten Abhilfemaßnahmen bzw. Sicherheitsvorkehrungen. Diese Datenschutz-Folgeabschätzung ist jedoch nur dann erforderlich, wenn eine geplanten Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten betroffener Personen birgt, insbes. bei Profiling oder umfangreicher Verarbeitung besonders sensibler Daten. Die DS-GVO sieht vor, dass die Aufsichtsbehörden zur Orientierung, wann ein hohes Risiko anzunehmen ist, – nicht abschließende – Listen von Verarbeitungen erstellen. Mit diesen Listen ist im Mai 2018 zu rechnen.

TOMs

Wie bisher sind dem ermittelten Risiko bzw. Schutzbedarf entsprechende technische und organisatorische Maßnahmen zum Schutz der Daten zu treffen. Neu sind dabei die Pflichten zu Maßnahmen zur Datenvermeidung (Protection by design) sowie zu Voreinstellungen bei der Entwicklung und Gestaltung von Produkten, Diensten und Anwendungen (Protection by default). Es müssen von vornherein Funktionen vorgesehen werden, die sicherstellen, dass die Verantwortlichen ihren Datenschutzpflichten nachkommen können.

Informationspflichten

Die DS-GVO stärkt die Rechte der Betroffenen und weitet insbesondere die Informationspflichten bei einer Datenerhebung erheblich aus. Zu statischen Erhebungen prüft der AKRdS gerade einen Anpassungsbedarf hinsichtlich der Unterrichtung nach § 17 BStatG. Soweit IT.NRW über den Statistikbereich hinaus Daten erhebt, müssen nun verständliche Informationen dazu erstellt werden.

Meldepflicht bei Datenpannen

Neu ist auch die Pflicht, jeden Datenschutzverstoß, durch den irgendwelche Beeinträchtigungen für die Betroffenen drohen, innerhalb von 72 Stunden der

Aufsichtsbehörde zu melden. Wenn mögliche Rechtsbeeinträchtigungen erheblich sind, müssen auch diese informiert werden. Weiter müssen alle Verletzungen des Schutzes personenbezogener Daten zukünftig fortlaufend dokumentiert werden, wobei die Fakten und Auswirkungen, die ergriffenen Gegenmaßnahmen und auch die Abwägung, ob LDI und/oder Betroffene zu informieren sind, beschrieben werden müssen. Die Meldepflicht gilt allerdings nicht für IT.NRW als Auftragsverarbeiter.

Auftragsverarbeitung

Wie bisher erfordert die Datenverarbeitung im Auftrag einen Vertrag, der nunmehr aber auch elektronisch geschlossen werden kann. Da die Inhalte umfangreicher geworden sind, sind auch zu den bestehenden Auftragsverhältnisse Nachträge zu vereinbaren. ZB 13 hat hierzu einen neuen Mustervertrag entworfen.