



SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz



Jetzt auf die Europäische Datenschutz-Grundverordnung vorbereiten

Bereits am 27. April 2016 wurde die Europäische Datenschutz-Grundverordnung (DS-GVO) verabschiedet. Sie ist bei der Verarbeitung personenbezogener Daten durch die Unternehmen ab dem 25. Mai 2018 unmittelbar anzuwenden. Bis dahin gilt das jetzige Bundesdatenschutzgesetz (BDSG). Da die DS-GVO einige Regelungsspielräume zugunsten des nationalen Gesetzgebers enthält, wird es auch ein noch zu änderndes BDSG und weitere spezielle Regelungen geben. Obwohl diese Vorschriften noch nicht abschließend feststehen, sollten sich die Unternehmen schon jetzt auf die Anwendung der DS-GVO vorbereiten, denn wesentliche Veränderungen stehen fest und die Umstellung auf die DS-GVO wird etwas Zeit beanspruchen. Gefordert sind hier Geschäftsführungen, betriebliche Datenschutzbeauftragte und Beschäftigte, die personenbezogene Daten verarbeiten. Was ist zu tun? Folgende Punkte sind besonders wichtig:

Befassung auf Leitungsebene

Datenschutz ist Chefsache. Die Organisation und Gesamtverantwortung für den Datenschutz liegt bei der Unternehmensleitung. Ihr obliegt es, Zuständigkeiten und Verantwortlichkeiten bezüglich der Anpassung des Datenschutzes an die DS-GVO festzulegen. Ggf. ist der Fortbildungsbedarf für den betrieblichen Datenschutzbeauftragten oder die Mitarbeiter, die die Datenverarbeitung durchführen, zu ermitteln. Die Erforderlichkeit bzw. die Anpassung von betriebsinternen Datenschutzrichtlinien ist zu prüfen. Existieren ausreichend Ressourcen in finanzieller, technischer und personeller Hinsicht oder besteht Bedarf an einer Unterstützung von außen? Verstöße beim Datenschutz können zu empfindlichen Folgen im Unternehmen führen. So wurden die Klagemöglichkeiten der betroffenen Personen erweitert. Der Bußgeldrahmen wurde drastisch erhöht. Nach wie vor kann es auch zu verwaltungsrechtlichen Verfahren kommen.

Änderungsbedarf ermitteln

Um den betriebsinternen Anpassungsbedarf zu ermitteln, sollte zunächst geprüft werden, in welchen Bereichen und durch welche Prozesse personenbezogene Daten verarbeitet werden. Die jetzt stattfindende Verarbeitung muss der Prüfung unterzogen werden, ob sie mit der DS-GVO vereinbar ist. Wichtig: Welche Verarbeitungen unterliegen welchen Risiken?

Rechtsgrundlage prüfen

Bevor personenbezogene Daten verarbeitet werden, sollte die Zulässigkeit der Verarbeitung geprüft werden. Dabei ist folgender Grundsatz zu beachten: die Verarbeitung personenbezogener Daten ist nur zulässig, wenn eine informierte und freiwillige Einwilligung der betroffenen Person oder eine gesetzliche Erlaubnisregelung dies gestattet (Art. 6 Abs. 1 DS-GVO).

Einwilligungen sind nicht wirksam, wenn deren Verweigerung zu Nachteilen für die betroffene Person führt (Erwägungsgrund 42). Problematisch sind sie in Über-/ Unterordnungsverhältnissen, z. B. im Beschäftigtenverhältnis (vgl. Erwägungsgrund 43). Zudem muss die betroffene Person darauf hingewiesen werden, dass durch den Widerruf der Einwilligung die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt ist.

Bei der Verarbeitung besonderer Kategorien personenbezogener Daten sind die Beschränkungen des Art. 9 DS-GVO zu beachten. Zu den besonderen Kategorien personenbezogener Daten gehören Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

Betroffenenrechte wahren

Die Betroffenenrechte haben in der DS-GVO wesentliche Veränderungen erfahren. Gänzlich neu sind das Recht auf Vergessenwerden und das Recht auf Datenübertragbarkeit.

Hat der Verantwortliche zu löschende Daten zuvor öffentlich bekannt gemacht, muss er angemessene Maßnahmen treffen, um die Verantwortlichen, die diese Daten verarbeiten, zu informieren, dass die betroffene Person Löschung verlangt hat, (Art. 17).

Nach dem Recht auf Datenübertragbarkeit müssen Daten auf Antrag der betroffenen Person ihm oder einem anderen in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden, wenn Verarbeitung automatisiert erfolgt und auf Einwilligung oder Vertrag nach Art. 6 Abs. 1b) beruht.

Zudem hat der Betroffene das Recht, in besonderen Situationen der Verarbeitung zu widersprechen, die u. a. auf einer Interessenabwägung nach Art. 6f DS-GVO beruht (gilt auch für Profiling). Folge des Widerspruchs ist, dass keine Weiterverarbeitung zulässig ist, es sei denn, das Überwiegen zwingender schutzwürdiger Gründe ist nachzuweisen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Wesentlich erweitert wurden die Informationspflichten, Art. 13, 14 DS-GVO, die mitunter schon bei der Erhebung personenbezogener Daten zu erfüllen sind. Insbesondere Datenschutzerklärungen sind hier zu überprüfen.

Datenschutz durch Technikgestaltung und durch datenschutzgerechte Voreinstellungen umsetzen

Schon bei Prozessgestaltung und Produktentwicklung ist zu prüfen, wie die Datenschutzgrundsätze - wie etwa die Datenminimierung - umgesetzt werden können. Durch Voreinstellungen in Produkten muss gewährleistet sein, dass nur solche personenbezogenen Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind.

Dokumentations-, Nachweis- und Meldepflichten beachten

Abgesehen von seltenen Ausnahmen muss ein Verzeichnis von Verarbeitungstätigkeiten geführt werden,

welches der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen ist, Art. 30 DS-GVO. Ein Vordruck wird auf der Homepage des Landesbeauftragten veröffentlicht.

Darüber hinaus ist der Unternehmer für die Einhaltung der Grundsätze der Datenverarbeitung (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit) im Rahmen der Rechenschaftspflicht nachweislichpflichtig, Art. 5 Abs. 2 DS-GVO.

Verletzungen des Schutzes personenbezogener Daten sind möglichst binnen 72 Stunden der Aufsichtsbehörde zu melden, Art. 33 DS-GVO. Besteht voraussichtlich ein hohes Risiko für die betroffene Person, ist sie unverzüglich zu benachrichtigen, Art. 34 DS-GVO.

Datenschutz-Folgenabschätzung implementieren

Hat eine Form der Verarbeitung ein hohes Risiko für die betroffene Person zur Folge, so ist vorab eine Datenschutz-Folgenabschätzung durchzuführen, Art. 35 DS-GVO. Sie ist insbesondere erforderlich bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten, z. B. Gesundheitsdaten, oder bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche. Geht aus der Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung ein hohes Risiko hätte und trifft das verantwortliche Unternehmen keine Maßnahmen zur Eindämmung des Risikos, so konsultiert es die Aufsichtsbehörde.

Verträge überprüfen

Verträge, die die Verarbeitung personenbezogener Daten betreffen, sollten überprüft und ggf. angepasst werden. Im Falle der Auftragsverarbeitung wären insbesondere die Art. 26-28 DS-GVO zu beachten. Auch Betriebsvereinbarungen und Tarifverträge sollten unter Berücksichtigung der noch bevorstehenden Verabschiedung des neuen BDSG überprüft werden.

Impressum

Herausgeber:

Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt
Leiterstr. 9, 39104 Magdeburg
Tel.: (0391) 81803-0
poststelle@lfd.sachsen-anhalt.de

www.datenschutz.sachsen-anhalt.de

Stand: Mai 2017