DSGVO-EVALUATION 2024

Positionspapier

Februar 2024

BvD e.V.

DATENSCHUTZ GESTALTEN

Gender-Hinweis:
Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen weiblich, divers und männlich (w/d/m) in diesem Text verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

BvD e.V.
DATENSCHUTZ GESTALTEN

IMPRESSUM

Herausgeber
Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.
Budapester Straße 31
10787 Berlin

T 030 . 26 36 77 60
F 030 . 26 36 77 63

bvd-gs@bvdnet.de
www.bvdnet.de

Stand
Februar 2024

AUF EINEN BLICK

Seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DSGVO) in allen Mitgliedstaaten der EU und des EWR verbindliches Recht. Ein wichtiger und richtiger Schritt! Datenschutz bedeutet Vertrauen und wird für viele Unternehmen zu einem Wettbewerbsvorteil.

Anlässlich der anstehenden zweiten Evaluierung der DSGVO im Jahr 2024 zeigt der BvD in diesem Papier auf, wie aus der Sicht der Datenschutzpraktiker die Wirtschaft – insbesondere kleine und mittlere Unternehmen (KMU) – bei der Erfüllung der datenschutzrechtlichen Anforderungen im Kontext der Digitalisierung noch besser unterstützt werden können.

1. **Querschnittskompetenz der Datenschutzbeauftragten – insbesondere in KMU – auch für mehr Datensicherheit nutzen.**
2. **Bürokratische Pflichten zum Schutz personenbezogener Daten risikobasiert ausgestalten.**
3. **Hersteller digitaler Lösungen und Dienste nach dem Verursacherprinzip in die Regelungen der DSGVO einbeziehen.**

1. Querschnittskompetenz der Datenschutzbeauftragten auch für mehr Datensicherheit nutzen – insbesondere in KMU

Betriebliche und behördliche Datenschutzbeauftragte (DSB) sind in Deutschland inzwischen seit mehr als einem halben Jahrhundert fest im Datenschutzrecht verankert. Sie sind mit ihrer Expertise die tragende Säule, um die mit den Geschäftsprozessen verbundene Verarbeitung von personenbezogenen Daten während des gesamten Datenlebenszyklus gesetzeskonform und unter Wahrung der Rechte der betroffenen Personen zu planen und durchzuführen.

In einer Zeit, in der Ransomware, Hackerangriffe- und Cyberattacken, Datenlecks und andere digital gesteuerte Angriffe auf öffentliche und nicht-öffentliche Stellen zunehmen, ist die Pflicht zur Benennung von Datenschutzbeauftragten ein wichtiges Instrument zum Schutz personenbezogener Daten, da Datenschutzbeauftragte auch Beratungsfunktionen hinsichtlich der Sicherheit der Verarbeitung personenbezogener Daten der verschiedenen Betroffenenkreise wahrnehmen. Durch interne Audits können Datenschutzbeauftragte auch die Wirksamkeit der ergriffenen Schutzmaßnahmen unabhängig überwachen und auf Verbesserungen hinwirken. Insbesondere in KMU ist die Vielseitigkeit der Datenschutzbeauftragten, die sich aus den fachlichen Anforderungen an die Qualifizierung für diese Rolle ergibt, ein Vorteil bei der Unterstützung der Unternehmensleitung. Ohne diese Querschnittskompetenz der Datenschutzbeauftragten drohen durch Angriffe auf die Sicherheit der Verarbeitung erhebliche gesamtwirtschaftliche Schäden. Denn gerade für KMU, die sich nicht immer mehrere verschiedene Fachberater „einkaufen“ können, stellt die themenübergreifende Fachkompetenz der Datenschutzbeauftragten eine Kostenersparnis dar.

Datenschutzbeauftragte sind Teil der Lösung, nicht des Problems

Unabhängig davon, ob ein Datenschutzbeauftragter benannt ist oder nicht, legt die DSGVO den Unternehmen, Behörden und anderen Stellen insbesondere mit den Artikeln 5, 24 und 32 DSGVO Pflichten bei der Verarbeitung personenbezogener Daten auf. Die Verantwortlichen sind aufgefordert, sowohl präventiv geeignete technische und organisatorische Maßnahmen (TOM) nach dem Stand der Technik umzusetzen als auch reaktiv diese zu überprüfen und zu aktualisieren. Dies erfordert eine den Anforderungen entsprechende Expertise und Erfahrung in der Organisation, die sich in der Querschnittskompetenz der Datenschutzbeauftragten manifestiert.

Datenschutzbeauftragte sind damit das Messwerkzeug im Werkzeugkasten der internen Selbstkontrolle für Unternehmen, Behörden und andere Stellen. Sie schützen diese vor dem Risiko, erst durch die ggf. sanktionsbewehrte behördliche Kontrolle der zuständigen Aufsichtsbehörde oder durch die Geltendmachung schadenersatzrechtlicher Ansprüche durch betroffene Personen auf Mängel und Fehler bei der Umsetzung des Datenschutzrechts aufmerksam zu werden. Gleichzeitig begrenzen Datenschutzbeauftragte durch ihre Beratung zu erforderlichen und angemessenen Schutzmaßnahmen Beeinträchtigungen durch Störungen der IT – sowohl von innen als auch von außen. Bei der Wahrnehmung ihrer gesetzlichen Aufgaben, insbesondere der Information und Beratung der obersten Managementebene, geben die Datenschutzbeauftragten wertvolle Impulse für die kontinuierliche Verbesserung der gesetzlich geforderten Datenschutzmaßnahmen, aber auch für die Angemessenheit dieser Maßnahmen. Mit ihrer Zuständigkeit für alle Fachbereiche, in denen Beschäftigte und Auftragsverarbeiter personenbezogene Daten verarbeiten, sind sie das Bindeglied, das die Einhaltung der Strategien zum Schutz personenbezogener Daten sowie der Datenschutzvorschriften überwacht und die Beschäftigten und Auftragsverarbeiter bei der Einhaltung der Vorgaben der Leitung berät.

Im Hinblick auf die immer wichtiger werdenden Digitalisierungsvorhaben sind die Datenschutzbeauftragten unverzichtbare Berater und Unterstützer für die Rechtmäßigkeit der geplanten Vorhaben. Ihre Beratung erfolgt bei frühzeitiger und sachgerechter Einbeziehung sowohl präventiv bei der Planung einer datenschutzkonformen Verarbeitung als auch reaktiv bei der Behebung von Mängeln.

2. Bürokratische Pflichten zum Schutz personenbezogener Daten risikoangemessen ausgestalten

Die DSGVO weist eine ausgeprägte Compliance-Methodik auf, die sich darin äußert, dass jede Zulässigkeitsprüfung durch Dokumentations- und Informationspflichten und jede Handlungspflicht durch Organisationspflichten flankiert wird.

So wird beispielsweise die Frage der Zulässigkeit einer Verarbeitung gemäß Art. 6 DSGVO flankiert von der Dokumentationspflicht nach Art. 5 Abs. 2 DSGVO (sog. Rechenschaftspflicht) und der Pflicht zur Angabe der Rechtsgrundlage gegenüber der betroffenen Person die Rechtsgrundlage nach Artt. 13, 14 DSGVO sowie der Pflicht zur Erfassung im Rahmen des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DSGVO. Damit löst selbst eine einfache Zulässigkeitsprüfung (z.B. die Verarbeitung der Kontodaten eines Beschäftigten zur Gehaltszahlung) drei weitere Pflichten aus. Hinzu kommt, dass diese flankierenden Pflichten nicht harmonisiert sind, sondern jeweils eine eigene Ausprägung hinsichtlich des Was und Wie der Dokumentation darstellen.

Jedes Unternehmen muss die Transparenz bei der Verarbeitung personenbezogener Daten gewährleisten. Dies bedeutet, dass die betroffene Person proaktiv umfassend über die Verarbeitung personenbezogener Daten informiert werden und ihr reaktiv auf Anfrage Auskunft erteilt werden muss. Nach der DSGVO sind diese Pflichten jedoch nicht nur zu erfüllen, sondern gemäß Art. 5 Abs. 2 i.V.m. Abs. 1 lit. a DSGVO muss auch dokumentiert werden, dass diese Pflichten erfüllt werden, und gemäß Art. 12 DSGVO müssen – unabhängig von der Unternehmensgröße – nachweislich Maßnahmen implementiert werden, um diese Transparenzpflichten zu erfüllen.

Festzustellen ist: Der eigentliche bürokratische und kostenintensive Aufwand durch die DSGVO besteht zu einem großen Teil darin, dass selbst einfach zu beurteilende Verarbeitungen personenbezogener Daten eine Vielzahl weiterer Pflichten und Aufwände auslösen. Diese Anforderungen bestehen für jedes Unternehmen – und zwar auch dann, wenn das Unternehmen keinen Datenschutzbeauftragten benannt hat.

Bürokratieentlastung von KMU: Vermeidung des Gießkannenprinzips

Es ist nicht so, dass dieser Mehraufwand unvermeidbar wäre. Schon das Bundesdatenschutzgesetz (BDSG) bot hinsichtlich der Frage nach der Zulässigkeit der Verarbeitung personenbezogener Daten kein geringeres Schutzniveau, kam aber ohne diese zusätzlichen Pflichten aus. Es lag daher in der Verantwortung des datenverarbeitenden Unternehmens, je nach Größe und Risiko der durchgeführten Verarbeitung personenbezogener Daten entsprechende Vorkehrungen zu treffen.

Eine Änderung der Pflicht zur Benennung eines Datenschutzbeauftragten würde an diesem bürokratischen Aufwand nichts ändern. Diese bußgeld- und schadensersatzbewehrten Pflichten sind in jedem Fall zu erfüllen. Verantwortlich dafür ist die jeweilige Unternehmensleitung. Ohne Datenschutzbeauftragten fehlt der Unternehmensleitung jedoch der „Kompass" durch die Bürokratie.

Ein wesentlicher Schritt zur Entlastung insbesondere der KMU ist es daher, den bürokratischen Überbau abzubauen und diese Pflichten nur risikoadäquat vorzusehen und sie nicht – ausgehend vom höchsten Schutzbedürfnis – nach dem Gießkannenprinzip auf alle Unternehmen anzuwenden. Gerade wenn sich die Umsetzung der Anforderungen am Risiko für die Rechte und Freiheiten der betroffenen Personen orientiert, können Datenschutzbeauftragte der geeignete „Lotse" sein.

3. Hersteller von digitalen Lösungen und Leistungen nach dem Verursacherprinzip in die Regelungen der DSGVO aufnehmen

Eine – wenn nicht die – wesentliche Herausforderung für die Anwender von Produkten zur Digitalisierung des Geschäftsalltags (seien es Apps oder andere digitale Lösungen und Dienste) besteht darin, dass die Hersteller durch die DSGVO nicht direkt in die Pflicht genommen werden. Die Beurteilung der datenschutzrechtlichen Anforderungen bleibt damit in der Verantwortung der Anwender hängen, auch wenn diese IT-seitig davon ausgehen, „Plug&Play"-Anwendungen zu erwerben. Der DSB ist dabei häufig der Überbringer der schlechten Nachricht, dass die gesetzlichen Anforderungen nicht erfüllt werden. Ein wesentlicher Ansatz zur Entlastung der KMU besteht daher darin, die Hersteller mit in die Pflicht zu nehmen. Die KMU müssen dann nur noch die Umsetzung in ihrem unternehmerischen Umfeld prüfen.

Die Binsenweisheit, dass ein Problem dort gelöst werden muss, wo es entsteht, hat die DSGVO mit Art. 25 DSGVO versäumt, umzusetzen. Denn wenn der Hersteller die Anforderungen des Datenschutzrechts nicht bereits bei der Entwicklung und Herstellung des Produkts die Anforderungen des Datenschutzrechts umsetzt, kann der Anwender mit einer solchen Anwendung auch nicht die Anforderungen der DSGVO erfüllen. Ein Beispiel hierfür ist Art. 25 Abs. 2 DSGVO: In der Praxis kann es für einen Verantwortlichen mitunter schwierig sein, der Pflicht zum Ergreifen geeigneter technischer und organisatorischer Maßnahmen nachzukommen. Häufig wird er nämlich gar nicht in der Lage sein, sinnvolle und ausreichende TOMs zu implementieren. Denn sowohl die dafür verwendete Hardware als auch - noch wichtiger - die Software werden in der Regel von einem externen Hersteller und nicht vom Verantwortlichen selbst bereitgestellt. Die TOMs, auf die der Verantwortliche Einfluss nehmen kann, beschränken sich häufig auf die Konfigurationen, die der Hersteller dem Nutzer seiner Software, dem verantwortlichen Unternehmen, freiwillig ermöglicht. Hinsichtlich dieser Konfigurationen gilt dann uneingeschränkt die Pflicht aus Art. 25 Abs. 2 DSGVO, die datenschutzfreundlichsten zu wählen - insgesamt bleibt der Schutz personenbezogener Daten aber auf der Strecke.

Vorbild KI-Verordnung: Hersteller zu TOMs verpflichten

Trotz der offensichtlichen Einflussmöglichkeiten des Herstellers auf die Ergreifung insbesondere technischer Maßnahmen, die er durch Voreinstellungen konfigurieren kann, lassen Wortlaut und Stellung der Norm im Kapitel „Verantwortlicher und Auftragsverarbeiter" keinen Zweifel daran, dass der Hersteller selbst nicht Normadressat oder aus anderen Gründen zur Ergreifung von TOMs verpflichtet ist.

Dabei handelt es sich jedoch nicht um ein redaktionelles Versehen. Denn der Hersteller wird durchaus erwähnt. So sieht Erwägungsgrund 78 Satz 3 der DSGVO vor, dass Hersteller sicherstellen sollten, dass Verantwortliche und Auftragsverarbeiter in der Lage sind, ihre datenschutzrechtlichen Pflichten zu erfüllen. Zudem wurde ein entsprechender Vorschlag des Europäischen Datenschutzbeauftragten (EDSB), zur Einbeziehung der Hersteller gerade nicht umgesetzt. Vor diesem Hintergrund besteht somit eine Verantwortungs- und Haftungslücke, die die Wirksamkeit des Art. 25 Abs. 2 DSGVO erheblich beeinträchtigt.

Nach dem Vorbild von Art. 24 der KI-Verordnung der Hersteller auch im Bereich des Datenschutzrechts zu TOMs verpflichtet werden. Damit würden die datenschutzrechtlichen Herausforderungen dort gebündelt, wo sie entstehen – am Anfang der Kette. Dies erleichtert es den Verantwortlichen, ihrerseits der Pflicht zur Ergreifung geeigneter TOMs nachzukommen.

In Art. 25 DSGVO sollte ein zusätzlicher Absatz eingefügt werden, der die Verantwortlichkeit der Hersteller explizit regelt; wobei idealerweise die Einheitlichkeit des Herstellerbegriffs mit dem der Produkthaftungsrichtlinie gewahrt werden sollte. Dies könnte durch Aufnahme einer entsprechenden Definition in Art. 4 DSGVO gewährleistet werden (so bereits der Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DSGVO aus dem November 2019, S. 16 f.).

Die Erfahrungen der letzten Jahre haben gezeigt, dass es notwendig ist, Art. 25 Abs. 2 DSGVO endlich zu einem wirksamen Instrument des Datenschutzes zu machen. Dazu ist es zwingend erforderlich, den Hersteller in den Adressatenkreis der Norm aufzunehmen und damit die derzeit bestehende Haftungslücke zu schließen. Dies würde zugleich eine Inanspruchnahme des Herstellers nach Artt. 82 und 83 Abs. 4 lit. a DSGVO ermöglichen.

WEITERE ANREGUNGEN

Bereits anlässlich der ersten Evaluierung der DSGVO im Jahr 2020 hatte der BvD Vorschläge erarbeitet, wie betriebliche und behördliche Datenschutzbeauftragte noch effektiver bei der Erfüllung datenschutzrechtlicher Anforderungen unterstützen können, sofern die dafür notwendigen regulatorischen Voraussetzungen geschaffen werden.

Siehe dazu: BvD-Positionspapier zur DSGVO-Evaluation 2020.

Über den Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Mit über 30 Jahren Erfahrung ist der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. die älteste Interessenvertretung für betriebliche und behördliche Datenschutzbeauf-tragte und -berater. BvD-Mitglieder sind in allen Branchen vertreten, insbesondere IT und IKT, Industrie/Produktion, Handel/Vertrieb, Beratung sowie Gesundheits- und Sozialwesen. Als erster Ansprechpartner der Betroffenen sind die BvD-Mitglieder Anlaufstelle für etwa fünf Millionen Arbeitnehmer sowie einen Großteil der Bürger und Konsumenten. Zudem sind sie als konstruktiv lösungsorientierte Datenschutzexperten ein wichtiger Partner für die verantwortliche Unternehmensleitung.

Die Verbandsvorstände, alle Leiter von Arbeitskreisen, Ausschüssen und Regionalgruppen des BvD bringen ihre praktische Erfahrung unentgeltlich in die Verbandsarbeit ein. Mit der Gründung des Europäischen Dachverbandes EFDPO (www.efdpo.eu) hat der BvD die Weichen für die verstärkte Vernetzung und Kommunikation auf EU-Ebene gestellt.

www.bvdnet.de