DSGVO-EVALUATION 2024

Positionspapier

5. September 2023

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
September 2023

AUF EINEN BLICK

Seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DSGVO) in allen EU- und EWR-Mitgliedsstaaten verbindliches Recht. Ein wichtiger und richtiger Schritt! Datenschutz steht für Vertrauen und wird für viele Unternehmen zum Wettbewerbsvorteil.

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

1. **Querschnittskompetenz von Datenschutzbeauftragten – insbesondere in KMU – auch für bessere Datensicherheit nutzen**
2. **Bürokratische Pflichten zum Schutz personenbezogener Daten risikoabhängig ausgestalten**
3. **Hersteller von digitalen Lösungen und Leistungen nach dem Verursacherprinzip in die Regelungen der DSGVO aufnehmen**

1. Querschnittskompetenz von Datenschutzbeauftragten auch für bessere Datensicherheit nutzen – insbesondere in KMU

Betriebliche und behördliche Datenschutzbeauftragte (DSB) sind in Deutschland inzwischen seit mehr als einem halben Jahrhundert im Datenschutzrecht fest verankert. Sie sind für Verantwortliche in öffentlichen und nicht-öffentlichen Stellen mit ihrer Expertise die tragende Säule, auf die diese bauen können, um die mit den Geschäftsprozessen einhergehende Verarbeitung von personenbezogenen Daten von Anfang bis Ende (Datenlebenszyklus) gesetzeskonform und unter Wahrung der Rechte der betroffenen Personen zu planen und durchzuführen.

In Zeiten akuter Ransomware-, Hacking- und Cyberangriffe sowie Leaks und sonstiger digital geführter Angriffe auf öffentliche wie auch nicht-öffentliche Stellen ist die Pflicht zur Benennung von Datenschutzbeauftragten ein wichtiges Instrument zum Schutz personenbezogener Daten von Bürgern, da die Datenschutzbeauftragten auch Beratungsfunktionen hinsichtlich der Sicherheit der Verarbeitung der personenbezogenen Daten der unterschiedlichen Betroffenenkreise übernehmen. Durch interne Audits können Datenschutzbeauftragte die Wirksamkeit der ergriffenen Schutzmaßnahmen auch überwachen und auch auf Verbesserungen hinwirken. Insbesondere in kleinen und mittleren Unternehmen (KMU) stellt die Vielseitigkeit von Datenschutzbeauftragten, welche sich aus den fachlichen Anforderungen an die Qualifizierung für diese Rolle ergibt, einen Vorteil für die Unterstützung der Unternehmensleitung dar. Ohne diese Querschnittskompetenz der gerade auch bei KMU tätigen Datenschutzbeauftragten droht durch erfolgreiche Angriffe auf die Sicherheit der Verarbeitung gesamtwirtschaftlich beträchtlicher Schaden. Denn gerade bei KMU, welche sich nicht immer mehrere verschiedene Fachberater „einkaufen“ können, stellt die nur für den DSB vorgesehene themenübergreifende Fachkompetenz eine Kostenersparnis dar.

DSB sind Teil der Lösung, nicht des Problems

Unabhängig davon, ob ein Datenschutzbeauftragter benannt ist, legt die DSGVO den Unternehmen, Behörden und sonstigen Stellen insbesondere mit den DSGVO-Artikeln 5, 24 und 32 Pflichten für die Verarbeitung personenbezogener Daten auf. Die Verantwortlichen sind gefordert, sowohl präventiv geeignete technische und organisatorische Maßnahmen (TOMs) umzusetzen, als auch reaktiv diese zu prüfen und zu aktualisieren. Dazu bedarf es einer den Anforderungen entsprechenden Expertise und Erfahrung innerhalb der Organisation, die sich in der Querschnittskompetenz der Datenschutzbeauftragten manifestiert.

Datenschutzbeauftragte sind damit das Messwerkzeug im Werkzeugkoffer der internen Selbstkontrolle für Unternehmen, Behörden und sonstigen Stellen. Sie schützen diese vor dem Risiko, erst durch die ggf. sanktionsbewährte behördliche Kontrolle der zuständigen Aufsichtsbehörde auf Mängel und Fehler in der Umsetzung des Datenschutzrechts hingewiesen zu werden. Gleichzeitig begrenzen die Datenschutzbeauftragten durch ihre Beratung zu erforderlichen und angemessenen Schutzmaßnahmen die Beeinträchtigung durch Störungen der IT – sowohl von innen als auch von außen. Datenschutzbeauftragte geben bei der Wahrnehmung ihrer gesetzlichen Aufgaben – also insbesondere der Unterrichtung und Beratung der obersten Managementebene – wertvolle Impulse für die kontinuierliche Verbesserung der gesetzlich geforderten Datenschutzmaßnahmen, aber auch zur 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 Beschäftigte und Auftragsverarbeiter zur Einhaltung der Vorgaben der Leitung berät.

Im Hinblick auf die ständig an Bedeutung zunehmenden Digitalisierungsvorhaben sind die Datenschutzbeauftragten unverzichtbare Berater und Unterstützer für die Rechtmäßigkeit der geplanten Vorhaben. Dabei fließt ihre Beratung bei frühzeitiger und ordnungsgemäßer Einbeziehung sowohl präventiv in die Planung der datenschutzkonformen Verarbeitung ein, als auch reaktiv bei der Behebung von Versäumnissen.

2. Bürokratische Pflichten zum Schutz personenbezogener Daten risikoangemessen ausgestalten

Die DSGVO weist eine ausgeprägte Compliance-Methodik aus, die sich darin niederschlägt, dass jede Zulässigkeitsbewertung durch Dokumentations- und Hinweispflichten und jede Handlungspflicht durch Organisationspflichten flankiert wird.

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

Jedes Unternehmen muss die Transparenz in Bezug auf die Verarbeitung personenbezogener Daten sicherstellen. Das bedeutet, dass die betroffene Person proaktiv umfassend über die Verarbeitung personenbezogener Daten informiert und ihr auf Verlangen reaktiv Auskunft erteilt werden muss. Nach der DSGVO müssen diese Pflichten jedoch nicht nur erfüllt werden, sondern nach Art. 5 Abs. 2 i.V.m. Abs. 1 lit. a DSGVO muss auch dokumentiert werden, dass diese Pflichten erfüllt werden, und nach Art. 12 DSGVO müssen – unabhängig von der Unternehmensgröße – nachweislich TOMs umgesetzt werden, um diese Transparenzpflichten zu erfüllen.

Festzustellen ist: Der eigentliche bürokratische und kostenintensive Aufwand durch die DSGVO besteht zum großen Teil darin, dass auch einfach zu bewertende und in jedem Unternehmen vorkommende Verarbeitungen personenbezogener Daten mehrere weitere Pflichten und Arbeitsaufwände auslösen.

Bürokratieentlastung von KMU: Vermeidung des Gießkannenprinzips

Es ist nicht so, dass diese zusätzlichen Aufwände unvermeidbar sind. Das vor der DSGVO geltende Bundesdatenschutzgesetz (BDSG) stellte in Bezug auf die Frage nach der (Un-)Zulässigkeit der Verarbeitung personenbezogener Daten keinen geringeren Schutz dar und kam dennoch ohne diese zusätzlichen Pflichten aus. Es lag damit in der Verantwortung des datenverarbeitenden Unternehmens, in Abhängigkeit von seiner Größe und des Risikos der ausgeführten Verarbeitung personenbezogener Daten entsprechende Vorkehrungen zu treffen.

Eine Änderung der Pflicht zur Benennung eines Datenschutzbeauftragten würde an dieser Bürokratie nichts ändern. Diese bußgeldbewehrten und auch zu Schadensersatzansprüchen führenden Pflichten müssen in jedem Fall erfüllt werden. In der Verantwortung hierfür steht die jeweilige Unternehmensleitung. Ohne Datenschutzbeauftragten fehlt der Unternehmensleitung jedoch der „Kompass“ durch die Bürokratie.

Ein wesentlicher Schritt zur Entlastung gerade von KMU besteht daher darin, den die eigentlichen Kernpflichten der DSGVO überladenden Bürokratieüberbau abzubauen und solche Pflichten nur risikoangemessen vorzusehen und sie nicht – ausgehend vom höchsten Absicherungsbedürfnis – nach dem Gießkannenprinzip auf alle Unternehmen anzuwenden. Gerade wenn die Umsetzung der Anforderungen am Risiko für die Rechte und Freiheiten der betroffenen Personen ausgerichtet wird, können Datenschutz-beauftragte den geeigneten „Kompass“ darstellen.

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

Eine – wenn nicht sogar die – wesentliche Herausforderung für Anwender von Produkten zur Digitalisierung des Unternehmensalltags (seien es Applikationen, seien es andere digitale Lösungen und Leistungen) besteht darin, dass die Hersteller durch die DSGVO nicht direkt in die Pflicht genommen sind. Die Bewertung der datenschutzrechtlichen Anforderungen bleibt damit in der Verantwortung der Anwender hängen, obgleich sie IT-seitig davon ausgehen, „Plug&Play“-Anwendungen zu kaufen. Der DSB ist dabei vielfach der Bote, der die schlechte Nachricht der fehlenden Erfüllung gesetzlicher Anforderungen überbringt. Ein wesentlicher Ansatz zur Entlastung der KMU besteht deshalb darin, die Hersteller mit in die Pflicht zu nehmen. Die KMU müssen dann nur noch den konkreten Einsatz 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 nicht bereits bei der Entwicklung und Herstellung des Produkts die Anforderungen des Datenschutzrechts umsetzt, kann der Anwender die Vorgaben der DSGVO mit einer solchen Anwendung auch nicht erfüllen.

Veranschaulichen lässt sich das anhand von Art. 25 Abs. 2 DSGVO: In der Praxis kann es sich für einen Verantwortlichen mitunter als schwierig erweisen, der Verpflichtung zur Ergreifung 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 bedeutsamer, die Software werden zumeist durch einen externen Hersteller und nicht den Verantwortlichen selbst bereitgestellt. Die TOMs, die der Verantwortliche beeinflussen kann, beschränken sich vielfach lediglich auf diejenigen Konfigurationen, die der Hersteller dem Verwender seiner Software, dem verantwortlichen Unternehmen, freiwillig ermöglicht. Bezüglich dieser Konfigurationen gilt dann natürlich uneingeschränkt die Pflicht aus Art. 25 Abs. 2 DSGVO, die datenschutzfreundlichsten zu wählen; insgesamt geht der Schutz personenbezogener Daten aber fehl.

Vorbild KI-Verordnung: Hersteller zu TOMs verpflichten

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

Um ein redaktionelles Versehen handelt es sich hierbei jedoch nicht. Denn der Hersteller findet durchaus Erwähnung. So ist im Satz 4 des Erwägungsgrundes 78 der DSGVO vorgesehen, dass Hersteller sicherstellen sollten, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Zudem war ein entsprechender Vorschlag des Europäischen Datenschutzbeauftragten (EDSB), die Hersteller miteinzubeziehen, eben gerade nicht umgesetzt worden. Es besteht vor diesem Hintergrund daher eine Verantwortungs- und Haftungslücke, aufgrund derer die Effektivität des Art. 25 Abs. 2 DSGVO stark beeinträchtigt ist.

Nach dem Vorbild der anstehenden KI-Verordnung (Art. 24 des entsprechenden Kommissionsvorschlags) sollte auch im Bereich des Datenschutzrechts der Hersteller zur Ergreifung von TOMs verpflichtet werden. Damit würden die Datenschutzherausforderungen dort akkumuliert, wo sie entstehen – am Anfang der Kette. Dies würde es den Verantwortlichen erleichtern, ihrerseits der Pflicht, geeignete TOMs zu ergreifen, nachzukommen.

In Art. 25 DSGVO wäre ein zusätzlicher Absatz anzufügen, welcher die Verantwortung der Hersteller explizit regelt; idealerweise sollte hierbei die Einheit des Herstellerbegriffs mit dem der Produkthaftungsrichtlinie gewahrt werden. Dies könnte durch Einführung einer dahingehenden Definition in Art. 4 DSGVO garantiert 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 geboten ist, Art. 25 Abs. 2 DSGVO endlich zu einem wirksamen Instrument des Datenschutzes zu machen. Dafür ist es zwingend erforderlich, den Hersteller in den Adressatenkreis der Norm einzubeziehen und somit die heute bestehende Haftungslücke zu schließen. Dies würde gleichzeitig auch eine Inanspruchnahme des Herstellers nach Artt. 82 und 83 Abs. 4 lit. a) DSGVO ermöglichen.

WEITERE ANREGUNGEN

Bereits anlässlich der ersten Evaluation der DSGVO in 2020 hatte der BvD Vorschläge erarbeitet, wie betriebliche und behördliche Datenschutzbeauftragte insbesondere KMU noch effektiver bei der Erfüllung datenschutzrechtlicher Anforderungen unterstützen könnten, sofern die dafür nötigen 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 Datenschutz-beauftragte 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