Gesellschaft für Datenschutz
und Datensicherheit (GDD) e.V.

GDD-Stellungnahme zur Entwicklung der DS-GVO

Nach Art. 97 Abs. 1 DS-GVO legt die EU-Kommission bis zum 25.05.2020 und danach alle vier Jahre dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung der Verordnung vor, der auch öffentlich gemacht wird. Im Zusammenhang mit dem Mitte 2024 fälligen zweiten Überprüfungsbericht führt die EU-Kommission derzeit eine Konsultation zur Evaluation der seit dem 1. Mai 2018 geltenden Datenschutz-Grundverordnung (DS-GVO) durch. Bis zum 8. Februar 2024 können Rückmeldungen bei der Kommission eingereicht werden. Zu berücksichtigen war dabei auch ein Fragebogen von September 2023, der zur Konsultation einer sog. High-Level-Expert-Group herangezogen wurde.

Die folgenden Ausführungen befassen sich mit der Bewertung einzelner Bereiche der DS-GVO, die von der GDD als besonders berücksichtigenswert erachtet werden:

1. Ausübung von Betroffenenrechten

Insgesamt sind sich die meisten Unternehmen durchaus bewusst, dass Betroffenenrechte geltend gemacht werden und dass die entsprechenden Anträge der Betroffenen auch zu erfüllen sind. Häufig sind sich allerdings weder die Betroffenen noch die Verantwortlichen im Klaren, in welchem Umfang die entsprechenden Rechte zu erfüllen sind. Das liegt unter anderem auch daran, dass den Betroffenen nicht immer bewusst ist, dass es sich bei den Betroffenenrechten nicht um absolute Rechte handelt, sondern dass bei der Erfüllung dieser Anträge stets eine Abwägung gegen Rechte anderer durch den Verantwortlichen erfolgen kann.

a) Informationspflichten, Artt. 13, 14 DS-GVO

Die durch den Verantwortlichen zu erfüllenden Informationspflichten nach Artt. 13 und 14 DS-GVO haben zu einem Übermaß an Informationen geführt, die von dem Betroffenen weder nachgefragt noch zur Kenntnis genommen werden. Durch diese in der Praxis vorherrschende Umsetzung der Informationspflichten wird dem Gebot der Transparenz keine Rechnung getragen, wenn der Verantwortliche nur darauf bedacht ist, seiner Rechtspflicht der Information nachzukommen. Demnach wäre es empfehlenswert, weitere Ausnahmen für Artt. 13 und 14 DS-GVO zu normieren und erwogen werden, Datenschutzerklärungen auf Internetseiten zu standardisieren.

Auch hinsichtlich des Informationszeitpunktes bestehen gewisse Unklarheiten und Unsicherheiten. Die Form- und Fristenregel des Art. 13 DS-GVO ist insbesondere im Hinblick auf die Erhebung personenbezogener Daten in konkreten Alltagssituationen wenig praktikabel. Im persönlichen Kontakt, beim Austausch von Visitenkarten, bei der Erstkontaktaufnahme per E-Mail oder der Erhebung von Daten am Telefon, verlangt der Wortlaut des Art. 13 DS-GVO das Bereitstellen der Information zum Zeitpunkt der Erhebung. Damit würde aber häufig der erste (persönliche) Kontakt mit bürokratischen Transparenzpflichten konterkariert. Abhilfe schaffen könnte eine kurze konkrete und ggf. mit Strafe bewehrte Frist.

b) Auskunftsanspruch, Art. 15 DS-GVO

Für Verantwortliche ist nicht eindeutig normiert, in welchem Umfang ein Auskunftsersuchen zu erfüllen ist. Das Recht auf Auskunft ist aufgrund seiner Kodifizierung in Art. 8 Abs. 2 S. 2 Grundrechte-Charta (GRCh) wohl als das zentrale Betroffenenrecht zu qualifizieren. Deswegen ist für die Gewährleistung dieses Rechts eine Konkretisierung der Unterschiede zwischen der „Auskunft über diese personenbezogenen Daten" (Art. 15 Abs. 1 S. 1 DS-GVO), der Auskunft über „die Kategorien personenbezogener Daten, die verarbeitet werden" (Art. 15 Abs. 1 S. 1 lit. b) DS-GVO) sowie die „Kopie der personenbezogenen Daten" (Art. 15 Abs. 3 S. 1 DS-GVO) geboten. Es ist in der Rechtspraxis nur schwer nachvollziehbar, wo der Unterschied in den vom Antragsteller erbetenen Auskünfte liegen soll. Gerade der Begriff der „Kopie" nach Art. 15 DS-GVO ist aufgrund einer fehlenden Legaldefinition oder mangels Konkretisierungen in den Erwägungsgründen der DS-GVO mit immenser Rechtsunsicherheit verbunden, da Verantwortliche derzeit nicht wissen, wie sie einem Antrag auf eine Kopie personenbezogener Daten entsprechen sollen. Die bereits in Erwägungsgrund 63 DS-GVO enthaltene Mitwirkung des Betroffenen, „dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht" sollte im beidseitigen Interesse des Verantwortlichen und der betroffenen Person in Art. 15 DS-GVO kodifiziert werden. Diese Anforderung der Präzisierung an die betroffene Person zur Mitwirkung bei der Beantragung der Auskunft sollte dabei zusätzlich noch spezifiziert werden. Diese Spezifizierung hätte auch zur Folge, dass die Verantwortlichen Klarheit darüber hätten, wann eine Anfrage einer betroffenen Person abgeschlossen ist.

Kleine und mittlere Unternehmen (KMU) benötigen für die Erteilung der Auskunft regelmäßig mehr Zeit. Das liegt zum einen daran, dass die Ressourcen der KMU regelmäßig beschränkt sind und diese häufig auf ausgelagerte Verarbeitungsmodelle angewiesen sind. Dementsprechend könnte über eine die Entwicklung einer Leitlinie zur DS-GVO-konformen Erfüllung des Auskunftsanspruchs für KMU ein richtiger Ansatz zur Unterstützung und Entlastung darstellen.

c) Löschung, Art. 17 DS-GVO

Dem Antrag auf Löschung kommt eine immer größere Bedeutung zu und von diesem wird durch die Betroffenen immer häufiger Gebrauch gemacht. Den Betroffenen fehlt allerdings oftmals das Bewusstsein, dass gewisse Daten aufgrund bestehender Aufbewahrungspflichten nicht vollständig gelöscht werden können. Außerdem müssen fast alle Löschungen manuell vorgenommen werden, um sicher zu gehen, dass auch tatsächlich alle Daten korrekt gelöscht wurden, wodurch viel Zeit und Ressourcen gebunden werden. Dahingehend wäre die Entwicklung von Leitlinien zur Löschung von nutzergenerierten Daten von Vorteil.

d) Einwilligung

Die Anforderungen an die „Informiertheit" bei einer Einwilligung i.S.d. Art. 6 Abs. 1 lit. a) DS-GVO ist konkretisierungsbedürftig und bedarf einer verständlichen Abgrenzung von der Informationspflicht i.S.d. Artt. 13 und 14 DS-GVO. Nach Art. 5 Abs. 1 lit. a) DS-GVO muss eine Verarbeitung personenbezogener Daten nicht nur rechtmäßig, sondern zudem auch transparent erfolgen. Den Anspruch der Transparenz bereits in den Rechtmäßigkeitstatbestand

einfließen zu lassen und zusätzlich den allgemeinen Informationspflichten zu entsprechen, schafft für die Rechtspraxis Schwierigkeiten, Einwilligungen rechtskonform einzuholen.

e) Datenübertragbarkeit

Das Recht auf Datenportabilität (Art. 20 DS-GVO) zielt darauf ab, dass der betroffenen Person sie betreffende Daten, die sie einem Verantwortlichen bereitgestellt hat, von dem Verantwortlichen in einem Format zur Verfügung gestellt werden, das die Übermittlung an einen anderen Verantwortlichen erlaubt. Dieses Betroffenenrecht verfolgt damit die Ermöglichung bzw. Erleichterung eines Anbieterwechsels. Im Vorschlag der Europäischen Kommission war hierzu in Erwägungsgrund 55 DS-GVO als Beispiel die Übertragung von einem sozialen Netzwerk auf ein anderes genannt worden. Im Hinblick auf den typischen Anwendungsfall von Art. 20 DS-GVO, der Umzug des eigenen Profils von einem Diensteanbieter im Internet (z.B. einem sozialen Netzwerk oder einem E-Mail-Provider) zu einem anderen, erscheint der Anwendungsbereich der Regelung des Art. 20 DS-GVO zu extensiv. Es erschiene deswegen sinnvoll den Anwendungsbereich auf (Online-)Portale zu begrenzen, um damit der ursprünglichen Zielsetzung dieser Regelung zu entsprechen. Das Recht auf Auskunft nach Art. 15 DS-GVO erfüllt auch bei Beschränkung des Anwendungsbereichs des Art. 20 DS-GVO weiter die Funktion dem Betroffenen auf Wunsch Transparenz über seine personenbezogenen Daten zu verschaffen.

2. Auftragsdatenverarbeitung, Art. 28 DS-GVO

Die Verarbeitung im Auftrag eines Verantwortlichen (Art. 28 DS-GVO) ist eine für die Rechtspraxis maßgebliche Rechtsfigur. Aus diesem Grund ist die konkrete Ausgestaltung der Regelung des Art. 28 DS-GVO für den Rechtsanwender von hoher Relevanz. Deswegen erscheint eine Klarstellung wünschenswert, dass die Schriftlichkeit einer Genehmigung von weiteren Auftragsverarbeitern nach Art. 28 Abs. 2 S. 2 DS-GVO auch elektronisch erfolgen kann. Die DS-GVO gestattet in Art. 28 Abs. 9 DS-GVO ein „elektronisches Format“ nur für Art. 28 Abs. 3 u. 4 DS-GVO. Für eine Vielzahl praxisrelevanter Auftragsverarbeitungen droht die durch Abs. 9 ermöglichte elektronische Form leerzulaufen. Dieser Umstand scheint der spezifischen Regelungsintention der Vorschrift zuwider zu laufen. Auch wenn bereits jetzt in der Rechtsanwendung richtigerweise davon ausgegangen wird, dass eine schriftliche Genehmigung im Sinne von Abs. 2 S. 1 DS-GVO auch im elektronischen Format erteilt und dokumentiert werden kann, sollte der Verordnungsgeber diese Regelungslücke in Art. 28 Abs. 9 DS-GVO nach Möglichkeit schließen. Dies würde auch über eine allgemein geltende Gleichstellung schriftlicher und elektronischer Form – wie in Art. 28. Abs. 9 DS-GVO – innerhalb der Begriffsbestimmungen in Art. 4 DS-GVO gelingen.

3. Datenschutzbeauftragte

Nach Art. 37 Abs. 1 lit. a) DS-GVO muss jede öffentliche Stelle unabhängig von der personellen Größe der Einrichtung und dem Risiko der darin verarbeiteten personenbezogenen Daten einen Datenschutzbeauftragten benennen. In der Privatwirtschaft bleibt die Bestellpflicht

eines Datenschutzbeauftragten hingegen lediglich die Ausnahme. Im Sinne einer konsistenten Fokussierung der DS-GVO auf den risikobasierten Ansatz erscheint die Übernahme einer Bestellpflicht für Datenschutzbeauftragte im nicht öffentlichen Bereich analog zur Bestellpflicht für öffentliche Stellen geboten. Eine solche Bestellpflicht lässt sich z.B. anhand der Parameter Unternehmensgröße (gemessen in Anzahl der Beschäftigten i.S.d. § 26 Abs. 8 BDSG) sowie Branche und der damit verbundenen Kritikalität der Datenverarbeitung gesetzlich regulieren, sofern keine pauschale Bestellpflicht für Unternehmen eingeführt werden soll. Eine umfänglichere Benennung von Datenschutzbeauftragten trägt zweifelsfrei zur besseren Gewährleistung der Umsetzung der Vorgaben aus der DS-GVO bei. Für die konkrete Aufgabenerfüllung durch Datenschutzbeauftragte erscheint eine Präzisierung der Aufgabe Überwachung (Art. 39 Abs. 1 lit. b) DS-GVO) wünschenswert, um diesen Terminus von der damit naheliegenden Aufgabe der Kontrolle abzugrenzen. Gegenwärtig verschwimmt die gesetzlich festgeschriebene Aufgabe der Überwachung mit einer Kontrollaufgabe in der Praxis häufig miteinander. Gem. Art. 39 DS-GVO ist der Datenschutzbeauftragte jedoch mit der Überwachung betraut, wozu u.a. die Überprüfung eines Kontrollsystems in der datenverarbeitenden Stelle gehören mag, aber nicht die Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften beim Verantwortlichen selbst gemeint sein soll. Hier ist eine Schärfung der Überwachungsfunktion legislativ geboten, um diese Aufgabe deutlicher herauszustellen und von der Kontrollfunktion abzugrenzen.

4. Bußgelder

Das mit der DS-GVO stark verschärfte Sanktionsregime schafft ein hohes Bewusstsein, die personenbezogene Datenverarbeitung rechtskonform zu gestalten und leistet damit einen bedeutsamen Beitrag zur Effektivierung des Rechts. Es bedarf aber einer gesetzlichen Klarstellung, dass eine Meldung nach Art. 33 DS-GVO oder eine Benachrichtigung nach Art. 34 Abs. 1 DS-GVO in einem Verfahren gegen den Meldepflichtigen oder Benachrichtigenden nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden darf. Es ist geboten, das absolute Beweisverwendungsverbot für Bußgeldverfahren wegen Verstößen nach Art. 83 DS-GVO gesetzlich ausdrücklich anzuordnen. Dies dient der Absicherung des verfassungsrechtlich fundierten Verbots, jemanden zur Selbstbezichtigung zu verpflichten und lässt sich als unionsrechtliche Verfahrensgarantie qualifizieren. Nur so ist das Spannungsverhältnis zu lösen, dass sich der Verantwortliche entweder selbst eines sanktionierbaren Datenschutzverstoßes bezichtigen muss oder aber gegen die Meldungs- und Benachrichtigungspflicht verstößt, die ihrerseits gem. Art. 83 Abs. 4 lit. a) DS-GVO sanktioniert werden kann.

5. Meldung von Datenpannen

Die Meldung einer Verletzung des Schutzes personenbezogener Daten muss nach Art. 33 Abs. 1 S. 1 DS-GVO innerhalb von 72 Stunden, nachdem dem Verantwortlichen die Verletzung bekannt wurde, erfolgen. In der Rechtspraxis hat sich diese kurze Meldefrist als sehr ambitioniert dargestellt. Um Sachverhalte unternehmensintern auf ihre Meldepflicht hin sorgfältig

und gewissenhaft bewerten zu können, erscheint eine Ausweitung der Meldefrist – auf z.B. 5 Tage (120 Stunden) – wünschenswert.

6. Gemeinsame Verantwortlichkeit

Die Rechtsfigur der gemeinsamen Verantwortlichkeit stellt für die Rechtspraxis eine enorme Herausforderung dar. Häufig wird im Falle der Ablehnung einer Verarbeitung im Auftrag nach Art. 26 DS-GVO eine gemeinsame Verantwortlichkeit i.S.d. Art. 26 DS-GVO unterstellt, die aber regelmäßig nicht vorliegt. Abseits der Schwierigkeit der Einordnung von Konstellationen mit mehreren Akteuren als gemeinsame Verantwortlichkeit wäre eine gesetzliche Klarstellung dahingehend hilfreich, dass der erfüllte Tatbestand einer gemeinsamen Verantwortlichkeit keine Rechtsgrundlage für den Datenaustausch zwischen den beteiligten Verantwortlichen darstellt. Der Datenaustausch zwischen mehreren Verantwortlichen bedarf einer Rechtmäßigkeit, die sich jedenfalls nicht allein aus Art. 26 DS-GVO ergibt. Die Rechtsfolgen einer gemeinsamen Verantwortlichkeit umfassen maßgeblich eine „Vereinbarung in transparenter Form“ (Art. 26 Abs. 1 S. 2 DS-GVO) sowie die grundsätzlich gesamtschuldnerische Haftung nach Maßgabe des Art. 82 DS-GVO, weil dort von „jedem an einer Verarbeitung beteiligten Verantwortlichen“ und „mehr als ein Verantwortlicher“ die Rede ist, somit also von einer Pluralität von Verantwortlichen ausgegangen wird. Aufgrund der vom Verordnungsgeber vorgenommenen Einordnung der Rechtsfigur der gemeinsamen Verantwortlichkeiten in das Kapitel der allgemeinen Pflichten von Verantwortlichen und Auftragsverarbeitern sollte die Regelung der Zusammenarbeit von mehreren Verantwortlichen teleologisch die Wahrung der Betroffenenrechte im Fokus haben. Maßgeblich sollte deswegen die Organisationspflicht dazu beitragen dem Betroffenen Klarheit zu schaffen, an welcher Stelle er wie seine Rechte ausüben kann. Die gemeinsame Haftung hingegen sollte in ihrer Reichweite vom Verordnungsgeber auf ein für die gemeinschaftliche Haftung adäquates Maß begrenzt werden. Schließlich besteht keine Transparenz für jeden der mehreren Verantwortlichen in die Datenverarbeitung der jeweils anderen Verantwortlichen, mit denen eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO besteht, was eine pauschal gesamtschuldnerische Haftung unverhältnismäßig erscheinen lässt. Deswegen würde z.B. eine Haftung i.S.d. „Ketten-Theorie“ der Rechtspraxis mehr entsprechen.

7. Kleine und mittlere Unternehmen (KMU)

Für KMU ist die Anwendung und Umsetzung der Vorgaben der DS-GVO im Regelfall nicht ohne externe Hilfe möglich. Das hängt insbesondere damit zusammen, dass sich die Vorschriften der DS-GVO oftmals im Rahmen der Bewertung der Maßnahmen von größeren Unternehmen ausgelegt und beurteilt werden. Werden diese Maßstäbe dann für alle Unternehmen herangezogen, können diese in einem Missverhältnis zu den Kapazitäten und Ressourcen der kleineren Unternehmen stehen. Für die KMU sind daher entsprechende Leitlinien des EDSB zu theoretisch und schwer umzusetzen. Oftmals ist externe Hilfe erforderlich, um den Anforderungen gerecht werden zu können. Eine Beratungsstelle für KMU bei den Datenschutzbehörden ist hilfreich, damit das Bewusstsein für die richtige Umsetzung der Vorgaben der DS-GVO erfolgen kann. So könnten zum Beispiel DS-GVO-Checkups angeboten werden,

die insbesondere kleineren Unternehmen zugutekommen könnte. Insgesamt ist der Schutz der personenbezogenen Daten mit der unternehmerischen Freiheit der KMU ins Gleichgewicht zu bringen.

8. DS-GVO und neue Innovationen

Die technologieneutrale Natur der Datenschutz-Grundverordnung kann nach Ansicht der GDD bei ihrer Anwendung auf innovative neue Technologien funktionieren. Die Datenschutzgrundsätze sind weit genug gefasst, um innovationsbasierte Datenverarbeitungsprozesse zu umfassen und entsprechend flexibel zu beurteilen. Insbesondere zwischen der KI-VO und der DS-GVO werden erhebliche Wechselwirkungen erwartet. Hier müssen mit Unterstützung des Europäischen Datenschutzausschusses (EDSA) konstruktive Best-Practice-Ansätze geschaffen werden.

9. Fazit

Insgesamt hat die DS-GVO wichtige Schutzmechanismen für die Privatsphäre geschaffen, aber ihre Umsetzung erfordert eine fortlaufende Anpassung, um die Bedürfnisse von Unternehmen und Bürgern gleichermaßen zu erfüllen. Gerade im Hinblick auf die Belange kleinerer Unternehmen ist größere Rücksicht zu nehmen. Viele kleinere Unternehmen sind aufgrund fehlender Ressourcen nicht in der Lage, die Vorgaben der DS-GVO so umzusetzen, wie es große Unternehmen, die regelmäßig als Maßstab für die Entwicklung von Leitlinien und Auslegungen der Vorschriften der DS-GVO herangezogen werden, bewerkstelligen. In vielen Bereichen – insbesondere bei den Betroffenenrechten – ist es erforderlich, ein Gleichgewicht zwischen dem Schutz der betroffenen Personen und der unternehmerischen Freiheit der Verantwortlichen zu erreichen. Das kann insbesondere dadurch erreicht werden, dass die Anforderungen und Grenzen der einzelnen Betroffenenrechte klarer definiert werden, um so eine reibungslose Erfüllung der Anträge durch die Verantwortlichen gewährleisten zu können.

Bonn, den 06.02.2024

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. tritt als gemeinnütziger Verein für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen - insbesondere auch die Datenschutzbeauftragten - bei der Lösung und Umsetzung der vielfältigen mit Datenschutz und Datensicherheit verbundenen rechtlichen, technischen und organisatorischen Anforderungen zu unterstützen.

Gesellschaft für Datenschutz und Datensicherheit e.V.
Heinrich-Böll-Ring 10, 53119 Bonn
info@gdd.de | www.gdd.de