Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD e.V. Heinrich-Böll-Ring 10 53119 Bonn

Der Landesbeauftragte für den Datenschutz und die
Informationsfreiheit Baden-Württemberg
Herrn Dr. Stefan Brink
Königstr. 10 a
70173 Stuttgart

Via Mail: **Evaluation@LfDI.bwl.de**

Bonn, 27.06.2019

GDD e.V.
T +49 228 96 96 75 00
F +49 228 96 96 75 25
info@gdd.de
www.gdd.de

#DSGVO wirkt (?) – 1 Jahr DSGVO – Praxiserfahrungen und Evaluation

Hiermit nimmt die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) zur Evaluierung der Datenschutz-Grundverordnung (DS-GVO) durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink, wie folgt Stellung:

Das Ziel der DS-GVO war die Vollharmonisierung der Regelungen bei der Verarbeitung personenbezogener Daten in allen Mitgliedstaaten der Europäischen Union (EU). Diese Zielvorgabe konnte jedoch mit der DS-GVO nicht vollumfänglich erreicht werden. Zwar stellt die Grundverordnung unmittelbar anwendbares Datenschutzrecht dar, gleichwohl sind die Mitgliedstaaten an vielen Stellen weiterhin in der Pflicht nationale Regelungen vorzusehen. Dies gilt im Besonderen für die Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. So gesehen, stellt die DS-GVO eine „hinkende Verordnung“ oder einen Hybrid aus Richtlinie und Verordnung dar.

Die umfänglichen Regelungen innerhalb der DS-GVO sind häufig mit dem Wunsch nach Konkretisierung und Spezifizierung verbunden, da der Rechtsanwender regelmäßig mit Unsicherheiten bei der Anwendung des sekundärrechtlichen Datenschutzrechts konfrontiert ist. Auch im Sinne der praktikablen Rechtsanwendung sollten eindeutige und allgemein verständliche Regelungen das Ziel sein, um nicht noch mehr Rechtsunsicherheit bei der Verarbeitung personenbezogener Daten zu erzeugen. Das ist mit Blick auf die Anwendung der DS-GVO im ersten Jahr ihrer Anwendungspflicht nicht gelungen.

Ausgewählte Regelungsbereiche in der Kritik

Aufgrund des Umfangs der DS-GVO sind die Ausführungen im Folgenden auf ausgewählte Regelungsbereiche der Grundverordnung beschränkt.

Datenschutz-Managementsystem

Die Einführung bzw. der Nachweis eines Datenschutz-Managementsystems überfordern sowohl Vereine als auch kleinere Unternehmen. Als Generalnorm weist Art. 24 DS-GVO dem Verantwortlichen den datenschutzrechtlichen Pflichtenkreis zu. Der Verordnungsgeber tut dies für jedwede Verarbeitung, die durch den Verantwortlichen, in seinem Namen oder für ihn erfolgt. Der Verantwortliche muss nicht nur geeignete und wirksame Maßnahmen zur Einhaltung der sich aus der DS-GVO ergebenden Pflichten treffen, vielmehr muss er auch nachweisen können, dass die Einhaltung dieser Pflichten sichergestellt ist. In Art. 24 DS-GVO finden sich leider auch keine konkreten Vorgaben darüber, welche Compliance- und Datensicherheitsmaßnahmen der Verantwortliche zu treffen hat. Es mangelt hier insbesondere an einer Differenzierung der Anforderungen nach Art. 24 DS-GVO, was zu einem immensen pauschalen Aufgabenmaß für jeden Verantwortlichen führt.

Informationspflichten

Inhalt
Die Informationspflichten gem. Art. 13 und 14 DS-GVO haben zu einem Übermaß an Informationen geführt, die vom Betroffenen weder nachgefragt noch interessiert zur Kenntnis genommen werden. Gerade die extrem langen und zumeist unübersichtlichen Hinweise in Form von Datenschutzerklärungen führen nicht zu einer von der DS-GVO beabsichtigten Transparenz auf Seiten des Betroffenen, sondern dienen allenfalls zur Erfüllung einer Rechtspflicht des Verantwortlichen. Es ist zu überlegen, weitere Ausnahmen für Art. 13 u. 14 DS-GVO zu normieren. In spezifischer Hinsicht sollte erwogen werden die Datenschutzerklärungen auf Internetseiten zu standardisieren.

Form
Eine gesetzgeberische Klarstellung würde dem in der Praxis bereits meist praktizierten sog. Medienbruch zur Rechtssicherheit verhelfen. Im Rahmen einer Videoüberwachung haben die deutschen Aufsichtsbehörden den Medienbruch für die Bereitstellung der Informationspflichten bereits als zulässig qualifiziert. Es wäre zu begrüßen, wenn die Legislative normiert, welche Informationen zwingend in einer 1. Stufe und welche Informationen erst in einer 2. Stufe bereitgestellt werden müssen.

Zeitpunkt der Informationserteilung
Insbesondere mit Blick auf die Erhebung personenbezogener Daten in konkreten Alltagssituationen ist die Form- und Fristenregel nach Art. 13 DS-GVO wenig praktikabel und nicht im Einklang mit dem ursprünglich verfolgten Zweck der Informationen. Im persönlichen Kontakt, beim Austausch von Visitenkarten, bei der Erst-Kontaktaufnahme 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.

Auskunftsrecht

Das Recht auf Auskunft ist aufgrund seiner Kodifizierung in Art. 8 Abs. 2 S. 2 GR-Charta 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 Auskünften liegen soll. Gerade der Begriff der „Kopie“ nach Art. 15 DS-GVO ist aufgrund einer fehlenden Legaldefinition oder mangels Konkretisierungen in den Erwägungsgründen (ErwGr) 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 ErwGr 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.

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. Art. 13 u. 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.

Datenportabilität

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 ErwGr 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.

Auftragsverarbeitung

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 auch in elektronischem Format erteilt und dokumentiert werden kann, sollte der Verordnungsgeber diese Regelungslücke in Art. 28 Abs. 9 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.

Datenschutzbeauftragter

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.

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 absolutes 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.

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.

Gemeinsam Verantwortliche

Die Rechtsfigur der Gemeinsamen Verantwortlichkeit stellt für die Rechtspraxis eine enorme Herausforderung darf. 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.

RA Andreas Jaspers, Geschäftsführer der GDD e. V.