Ausgewählte Anforderungen der EU-DSGVO an die Verarbeitung personenbezogener Daten

Klaus Gennen[1]

Abstract: Die EU-Datenschutz-Grundverordnung, die einen EU-einheitlichen Schutz personenbezogener Daten (pbD) bewirken soll, ist ab dem 25.5.2018 zwingend anzuwenden. Es wird mit Wirkung für diejenigen Bereiche der Landwirtschaft, in denen personenbezogene Daten anfallen bzw. verarbeitet oder genutzt werden, Paradigmenwechsel geben. So steigen die Dokumentationspflichten erheblich an. Ferner wird der Verantwortliche künftig in dem Sinne rechenschaftspflichtig sein, dass er die Einhaltung der datenschutzrechtlichen Vorschriften zu beweisen hat, bei der Auftragsverarbeitung kommen mehr Verpflichtungen auf die Beteiligten zu, die Bußgelder bei Verstößen steigen exorbitant. Hersteller werden mehr Wert auf Privacy by Design bzw. Privacy by Default legen müssen. Unternehmen, in denen pbD anfallen, sollten, um auf die Umstellung der Rechtsordnung vorbereitet zu sein, bald mit einem entsprechenden Projekt beginnen.

Keywords: EU-Datenschutz-Grundverordnung, räumlicher Anwendungsbereich, Dokumentationspflicht, Privacy by Design/by Default, Rechenschaftspflicht, Bußgeld, Auftragsverarbeitung, Arbeitnehmerdatenschutz.

1 Einleitung

Die Nutzung von Technologien, deren Anwendung personenbezogene Daten („pbD“) erzeugt bzw. die pbD verarbeiten, ist aus Land-/Forstwirtschaft nicht wegzudenken. Insbesondere entstehen pbD, wenn Arbeitnehmer/Beschäftigte (z.B. bei Lohnunternehmen) oder Landwirte Geräte mit elektronischer Steuerung/Überwachung bei Precision Agriculture/Foresting oder ähnlichen Arbeiten benutzen. Wann immer sich bei oder nach Benutzung einer Maschine ohne besondere Schwierigkeiten Rückschlüsse auf einen konkreten Benutzer ziehen lassen, liegen wahrscheinlich pbD vor. Auch die Hersteller solcher Maschinen bzw. die herstellergebundene oder freie Wartungsorganisation haben ein Interesse an solchen Daten, um Auskünfte über die Maschinen (und ggf. deren Benutzer, z.B. beim Verkauf gebrauchter Maschinen oder beim Verleih) zu gewinnen – geschieht dies nicht anonymisiert, liegen pbD vor.

Die Datenschutz-Grundverordnung (DSGVO)[2] ist am 25.5.2016 in Kraft getreten und ist ab dem 25.5.2018 in den EU-Mitgliedsstaaten zwingend anzuwenden. An diesem Tag wird ein Schalter umgelegt und es wird einen in Teilen neuen Rechtsrahmen für den

[1] Rechtsanwalt u. Partner der Kanzlei LLR, Fachanwalt für IT-Recht und für Arbeitsrecht, ext. Datenschutzbeauftragter, Mevissenstr. 15, 50668 Köln, zugl. ordentl. Professor an der TH Köln, klaus.gennen@llr.de

[2] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Abl. EG L 119/1 v. 4.5.2016.

Schutz von pbD in der EU geben bzw. auch für Teile des grenzüberschreitenden Datenverkehrs.

2 Einige grundlegende Unterschiede zwischen BDSG und DSGVO

2.1 Räumlicher Anwendungsbereich

Nach Art. 3[3] ist die DSGVO nicht nur anwendbar auf Verantwortliche, die eine Niederlassung innerhalb der EU haben, sondern z.B. auch auf Unternehmen, die außerhalb der EU niedergelassen sind, aber mit ihren Produkten auf dem EU-Markt vertreten sind und dabei pbD verarbeiten. Auch diese müssen künftig die DSGVO einhalten, was eine Ausdehnung des Anwendungsbereichs über die EU-Grenzen hinaus bedeutet, z.B. beim Betrieb von Hersteller-Plattformen räumlich außerhalb der EU, auf denen nicht anonymisierte Anwendungsdaten von Benutzern aus der EU gesammelt werden. Der Gesetzgeber hat sich somit vom Territorialprinzip ab- und dem Marktortprinzip zugewandt.

2.2 Rechenschaftspflichten des Verantwortlichen, Dokumentation

Die DSGVO postuliert (z.B. Art. 5 Abs. 2, Art. 82 Abs. 3) umfassende Nachweis- und Rechenschaftspflichten des Verantwortlichen und des Auftragsverarbeiters. Der Verantwortliche, in den o.a. Fällen zumeist der Eigentümer oder Mieter der Maschine, muss nicht nur sicherstellen, dass er die Anforderungen der DSGVO erfüllt, sondern die Einhaltung im Zweifel auch gegenüber der Aufsichtsbehörde oder einem Geschädigten nachweisen können. Damit liegt die Verpflichtung, sich bei behaupteten Verstößen zu entlasten, künftig beim Verantwortlichen bzw. Auftragsverarbeiter. Diese Verpflichtung führt unmittelbar dazu, dass Unternehmen frühzeitig beginnen, ihr Datenschutzmanagementsystem („DSMS“) umzustellen bzw. ein solches DSMS einzuführen, um auch ein Organisationsverschulden zu vermeiden. Diese Aktivitäten erfolgen insbesondere wegen der erheblich erhöhten Bußgelder bei Verstößen (vgl. Ziff. 0). Die Aufsichtsbehörden, insbesondere die BfDI, sind derzeit dabei, ihr Personal aufzustocken, um besser als bisher ihrer gewandelten Aufsichtsfunktion und den weiteren Aufgaben der DSGVO gerecht werden zu können.

Zudem sieht die DSGVO auch eine umfangreichere Dokumentationspflicht vor (vgl. insbes. Art. 32) als das BDSG. Handelt es sich z.B. um einen Datenverarbeitungsvorgang, der ein hohes Risiko für die Sicherheit von pbD begründet, so ist eine Datenschutz-Folgenabschätzung (Art. 35) durchzuführen, die nicht mit der Vorabkontrolle nach dem BDSG verwechselt werden darf, und hieraus sind die entsprechenden Schutzmaßnahmen abzuleiten. Unter der DSGVO begründet ein Verstoß gegen Art. 35 Abs. 1 einen Buß-

[3] Artikelbezeichnungen ohne Benennung der rechtlichen Grundlage sind solche der DSGVO.

geldtatbestand. Nach Art. 32 ist ein Datensicherheitskonzept zu erstellen, auch die Informationspflichten gegenüber dem Betroffenen haben sich erhöht (Art. 12 ff).

2.3 Aufweichungen des Zweckbindungsgrundsatzes

Unter dem BDSG gilt ein eher strenger Zweckbindungsgrundsatz. Danach dürfen pbD im Grundsatz nur zu dem Zweck verwendet werden, für den sie erhoben wurden bzw. der Betroffene seine Einwilligung erteilt hat. Unter der DSGVO wird dieser Grundsatz etwas aufgeweicht, aber es bleibt grundsätzlich dabei, dass der Verantwortliche feststellen muss, ob ein Privilegierungstatbestand oder eine zulässige Zweckänderung vorliegt. Er muss also prüfen, ob die DSGVO die Nutzung zu einem anderen als dem ursprünglichen Zweck zulässt. Dabei werden (vgl. Art. 6 Abs. 4 lit. a) weitere Zwecke, die mit dem ursprünglichen Zweck „vereinbar" sind, als zulässig angesehen, wobei wiederum vereinbar „jede Verbindung" zwischen bisherigem und neuem Zweck sein soll. Insoweit wird man abwarten müssen, welche „Verbindung" aus Sicht von Unternehmen, die Interesse an den pbD haben, künftig ausreichen werden, und wie die Aufsichtsbehörden mit dem mit Sicherheit einsetzenden Wunsch, hierzu jede denkbare Verbindung ausreichen zu lassen, umgehen werden.

2.4 Neue Regelungen zur Auftragsverarbeitung, gemeinsame Verantwortlichkeit

Die Auftragsdatenverarbeitung nach § 11 BDSG wird zur Auftragsverarbeitung nach Art. 28 DSGVO. Der Begriff der Funktionsübertragung entfällt. Eine Verpflichtung zum schriftlichen Abschluss des Vertrages besteht nicht mehr, die elektronische Form reicht aus. Es bleibt bei dem Grundsatz, dass der Auftragnehmer weiterhin nur nach (zu dokumentierender) Weisung des Auftraggebers handeln darf. Die Auftragsverarbeitung bedingt eine vorherige Risikoabwägung nach Art. 32, der Katalog der technisch-organisatorischen Maßnahmen nach §§ 9, 11 BDSG i.V.m. der Anlage zu § 9 BDSG ist insoweit ersetzt worden durch das Datensicherheitskonzept. Den Auftragsverarbeiter treffen Verpflichtungen zur Unterstützung des Verantwortlichen. Je nach Art und Intensität eines Verstoßes gegen Art. 28 ist auch der Auftragsverarbeiter schadensersatzpflichtig bzw. bußgeldpflichtig. Verstößt der Auftragsverarbeiter gegen eine Weisung und bestimmt er selbst die Mittel der Verarbeitung, gilt er selbst als Verantwortlicher.

Zwar entfallen dem Wortlaut nach Erstkontrolle und laufende Kontrolle nach § 11 BDSG, aber aufgrund der umfassenden Rechenschaftspflicht wird der Verantwortliche künftig solche Kontrollen durchführen, zumal nach Art. 32 Abs. 1 lit. d. ein Verfahren zur regelmäßigen Kontrolle Teil des Datensicherheitskonzepts sein muss.

Nach Art. 27 besteht nun die Möglichkeit, dass sich mehrere Verantwortliche die Verantwortung teilen, damit steht ein weiteres Instrument zur Verfügung für die Zusammenarbeit mehrerer Beteiligter unter Verarbeitung von pbD.

2.5 Besonderheiten des Arbeitnehmerdatenschutzes

Die DSGVO verzichtet bewusst auf EU-weite Regelungen zum Arbeitnehmerdatenschutz (Art. 88). Vielmehr sollen die Mitgliedsstaaten den Arbeitnehmerdatenschutz selbst regeln. Lediglich in Erwägungsgrund 48 zur DSGVO wird angedeutet, dass eine konzerninterne Verarbeitung von Arbeitnehmerdaten (und Kundendaten!) von einem berechtigten Interesse des Verantwortlichen gedeckt sein kann. Der Referentenentwurf des BMI (Stand: 23.11.2016) zum Gesetz zur Anpassung des Datenschutzrechts sieht dementsprechend in Art. 1 Teil 2 Kap. 1 Abschnitt 2, § 24 die Fortschreibung der aktuellen Rechtslage vor, also des § 32 BDSG. Zudem bleiben betriebsverfassungsrechtliche Maßgaben, vgl. § 87 Abs. 1 Nr. 6 BetrVG, unberührt. An der bestehenden Rechtslage zum Arbeitnehmerdatenschutz ändert sich also, geht man von dem o. a. Referentenentwurf aus, praktisch nichts.

2.6 Privacy by Design/Privacy by Default

Art. 25 zwingt zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Wer Software zur Maschinensteuerung entwirft, muss sich künftig von Gesetzes wegen Gedanken darüber machen, wie Funktionen auch ohne pbD oder nur mit pseudonymisierten oder anonymisierten pbD oder unter Nutzung nur eines technisch notwendigen Minimums ans pbD ausgeführt werden können, weil Verantwortliche künftig solche Parameter zu berücksichtigen haben. Entsprechendes gilt für datenschutzfreundliche Voreinstellungen an bestehenden oder neuen Systemen.

2.7 Bußgeldtatbestände und Bußgeldhöhe

Wer Datenschutz bisher als Kostenfaktor ansehen hat, wird auf die neuen Bußgeldregelungen schauen. Von krassen Fällen abgesehen, waren die Bußgelder unter dem BDSG eher niedrig. Das wird sich unter der DSGVO erheblich ändern, sowohl im Hinblick auf die Anzahl der sanktionierten Tatbestände wie in Bezug auf die Bußgeldhöhe.

Bei Verstößen gegen die in Art. 83 Abs. 4 a) bis c) genannten Pflichten (z.B. fehlerhafte Auftragsverarbeitung) fallen Geldbußen von bis zu 10 Mio. Euro oder in Höhe von 2% des weltweiten Vorjahresumsatzes an. Liegt ein Verstoß gegen eine der in Art. 83 Abs. 5 a) bis e) normierten Pflichten vor (z.B. fehlende Einwilligung), geht es um bis zu 20 Mio. Euro oder 4%. Bisher noch ungeklärt ist die Frage, ob bei Konzernkonstellationen der Umsatz der Gruppe oder des betroffenen Unternehmens zugrunde zu legen ist. Je nach Größe der Unternehmensgruppe kann dies die Insolvenz einzelner Unternehmen bedeuten. Bei der konkreten Bußgeldbemessung werden die in Art. 83 Abs. 2 aufgezählten Kriterien berücksichtigt, z.B. das Ausmaß des Verschuldens. Im Übrigen werden die Sanktionen nach Art. veröffentlicht, was neben den finanziellen Schäden auch einen erheblichen Imageschaden für das betroffene Unternehmen und sogar die gesamte Unternehmensgruppe bedeuten kann.