Datenschutz durch Technik

Daten dürfen nur verarbeitet werden, wenn es dafür eine Rechtsgrundlage gibt. Soweit eine solche vorhanden ist, muss der Verantwortliche bestimmte Grundsätze beachten, darf beispielsweise die Daten nur zu bestimmten Zwecken verwenden und sie nicht an beliebige Dritte weitergeben oder ins Netz stellen. Doch reicht das für einen wirksamen Datenschutz? Gefahren gehen nicht nur von einem illoyalen Verarbeiter aus. Vielmehr können auch Dritte ein Interesse haben, auf die Daten zuzugreifen oder sie zu vernichten. Kann das Datenschutzrecht auch dagegen schützen? Sind dabei technische Vorkehrungen nicht vielleicht wirksamer als Verbote, die immer übertreten werden können?

von **Wolfgang Däubler**

Jedes Risiko von Datenmissbrauch ausschließen zu wollen, ist wenig realistisch. Niemand kann damit rechnen, dass die (sehr guten) Grundsätze des Art. 5 DSGVO immer zu hundert Prozent befolgt werden, beispielsweise volle Transparenz für die betroffene Person besteht und jedes überflüssig gewordene Datum sofort gelöscht wird. Insoweit geht es von vorne herein nur um eine möglichst weitgehende Annäherung an das Ideal, um eine Minimierung von Risiken.

Ein ganz wesentliches Mittel, wie man illegalen Umgang mit Daten verhindert, ist die Technik. Führt sie dazu, dass bestimmte Daten überhaupt nicht entstehen oder automatisch gelöscht werden, kommt es letztlich nicht auf den guten Willen oder die Angst vor Sanktionen bei einzelnen Menschen an. Die Wirkung ist anders als bei sonstigen Regeln von vorne herein gesichert.[1]

Die DSGVO sieht vier Wege vor, wie man zu einer „datenschutzfreundlichen“, risikoarmen Technik kommen kann.
- Nach Art. 25 Abs. 1 DSGVO ist der Verantwortliche verpflichtet, durch die Gestaltung der Technik dafür zu sorgen, dass möglichst wenige personenbezogene Daten zur Entstehung kommen. Man spricht insoweit von „privacy by design“.

[1] Vgl. Jandt DuD 2017, 562.

- Daran schließt Art. 25 Abs. 2 DSGVO an: Der Verantwortliche muss für „datenschutzfreundliche Voreinstellungen“ sorgen, also dafür, dass die Möglichkeiten eines Systems nur insoweit genutzt werden dürfen als dies unbedingt erforderlich ist. Für dieses Phänomen hat sich der Ausdruck „privacy by default“ eingebürgert.
- Die effektiv anfallenden („unvermeidlichen“) Daten müssen nach Art. 32 DSGVO gegen den unbefugten Zugriff Dritter gesichert sein. Andernfalls könnte der Betroffene nicht mehr erkennen, was mit seinen Daten geschieht und zu welchen Zwecken sie verwendet werden. Zu einem wirksamen Datenschutz gehört die Datensicherung.
- Unter bestimmten Voraussetzungen muss nach Art. 35 DSGVO eine sog. Datenschutz-Folgenabschätzung stattfinden. Dabei muss danach gefragt werden, welche Risiken sich für die betroffenen Personen aus einer bestimmten Datenverarbeitung ergeben. Je sensibler die Daten, umso ausgeprägter müssen die Schutzmechanismen sein. Die Datensicherung kann auf diese Weise eine Ergänzung erfahren.

Datenminimierung („Privacy by Design“)

Die Erhebung und Verarbeitung von Daten muss nach Art. 5 Abs. 1 Buchst. c DSGVO auf „das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.“ Das damit zum Ausdruck gebrachte Prinzip der Datenminimierung wird durch Art. 25 Abs. 1 DSGVO konkretisiert.[2] Dieser verpflichtet den Verantwortlichen zu technischen und organisatorischen Maßnahmen, die „dafür ausgelegt sind“, u. a. möglichst wenige Daten zur Entstehung zu bringen. Bislang war dasselbe Prinzip unter dem Stichwort der „Datenvermeidung“ in § 3a Satz 1 BDSG-alt niedergelegt worden.

Die praktische Bedeutung der Vorschrift des § 3a hielt sich sehr in Grenzen. Zwar wurde sie nach Kenntnis des Verfassers in zahlreichen Betriebsvereinbarungen erwähnt, doch sind in der Literatur so gut wie keine Fälle dokumentiert, in denen sich konkrete Konsequenzen ergaben. Dies mag damit zusammenhängen, dass ein Verstoß gegen § 3a BDSG-alt keine Sanktionen zur Folge hatte – das Bußgeld nach § 43 BDSG-alt beschränkte sich auf andere Tatbestände. Dies ändert sich nunmehr, da Art. 83 Abs. 4 Buchstabe a DSGVO auch für Verstöße gegen Art. 25 ein Bußgeld vorsieht, das bis zu 10 Mio. Euro oder bis zu 2 % des Weltumsatzes ais dem letzten Geschäftsjahr betragen kann. Schon aus diesem Grund muss das Prinzip der „privacy by design“ sehr viel ernster genommen werden.

[2] Heberlein, in: Ehmann/Selmayr Hrsg.), Kommentar zur DSGVO, 2017, Art. 5 Rn. 22 f.

Ein praktische Schwierigkeit ergibt sich allerdings dadurch, dass sich die DSGVO nicht an die Hersteller der fraglichen Geräte wendet.[3] Der Verantwortliche ist als solcher in der Regel darauf beschränkt, auf dem Markt ein Gerät zu kaufen, an dessen datenschutzfreundlicher oder datenschutzunfreundlicher Entwicklung er nicht beteiligt war.[4] Kann man ihm einen Vorwurf machen, wenn es auf dem Markt nur Geräte gibt, die die technischen Möglichkeiten zur Datenminimierung nicht im Entferntesten ausschöpfen? Ist es anders, wenn es zwar „datensparsame" Geräte gibt, diese aber im Preis sehr deutlich über den anderen liegen? Bisher ist dies – soweit ersichtlich – in der Literatur nicht problematisiert worden.

Es liegt nahe, eine Parallele zum Gesundheitsschutz zu ziehen. Wer Maschinen oder andere Geräte in Verkehr bringt, muss den Anforderungen des Produktsicherheitsgesetzes[5] genügen. Bei einem Einsatz als Arbeitsmittel erfolgt eine erneute Überprüfung nach der Betriebssicherheitsverordnung.[6] Etwas Vergleichbares fehlt im Datenschutz. Natürlich hat die Gesundheit höheren rang, doch schließt dies eine Ausdehnung nicht aus. müsste es auch im Datenschutz geben; beides ließe sich im Übrigen vom Verfahren her verbinden, so dass ein Zusatzaufwand für die öffentliche Hand und mögliche Verzögerungen bei der Produktion weithin vermieden würden.

Trotz dieser unbefriedigenden Rahmenbedingungen sind Fälle denkbar, in denen Art. 25 Abs. 1 DSGVO praktische Bedeutung gewinnen kann. In vielen Betrieben gibt es Automaten, aus denen sich die Beschäftigten jederzeit Getränke und einen kleinen „Snack" holen können. Müssen sie dabei mit dem Betriebsausweis bezahlen, lassen sich die Ess- und Trinkgewohnheiten bestimmter Personen unschwer ermitteln. Stattdessen kann man sich aber auch Karten ohne Personalnummer vorstellen, die man an einem „Geldautomaten" auflädt. Von dem dort befindlichen „Guthaben" wird dann der Preis der Ware abgebucht. Personenbezogene Daten entstehen dabei nicht – ganz wie es Art. 25 Abs. 1 DSGVO will. Nur: Die aktuellen Probleme lassen sich damit nicht einfangen.

Datenschutzfreundliche Einstellung („privacy by default")

[3] Jandt, DuD 2017, 563
[4] Nur wer insbesondere als Großunternehmen eine individuelle Software erstellen lässt, befindet sich in einer anderen Situation.
[5] v. 8.11.2011, BGBl I S. 2178, 2179; BGBl 2012 I S. 131, zuletzt geändert durch VO v. 31.8.2015 (BGBl I S. 1474)
[6] Dazu Däubler, Digitalisierung und Arbeitsrecht, 2018, § 6 Rn. 22 ff. (im Erscheinen)

Die Ausklammerung der Produzenten ist weniger gravierend, wenn es um die Deaktivierung bestimmter Merkmale geht. Art. 25 Abs. 2 DSGVO verlangt geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Zweck erforderlich sind. Sieht beispielsweise eine Telefonanlage ein Merkmal „Weiterleitung“ vor, so dass das Gespräch immer dort ankommt, wo sich die fragliche Person innerhalb des Betriebs gerade befindet, so lässt sich ansatzweise ein „Bewegungsprofil“ erstellen. Besteht dafür wie in der Regel keine Rechtfertigung, so ist entweder auf die Aktivierung der Weiterleitungsfunktion völlig zu verzichten oder aber sie ist in das Belieben des Beschäftigten zu stellen. Weiter wird vorgeschlagen, dass die Hersteller ihre Software mit abgestellter Protokollierungsfunktion ausliefern müssen.[7] Bei Bedarf und datenschutzrechtlicher Legitimation kann diese dann vom Käufer aktiviert werden.

Diese Grundsätze bestätigen, dass der Arbeitgeber als Verantwortlicher auch in einer Bewerbungssituation zur Konzentration auf das Notwendige verpflichtet ist. Bei jeder Informationserhebung ist daher zu prüfen, ob die abgefragten Daten im Hinblick auf die Eignung für die in Aussicht genommene Stelle wirklich erforderlich sind oder ob eine sachgerechte Entscheidung auch ohne sie möglich wäre. Damit ist nichts prinzipiell Neues festgelegt. Vielmehr geht es um eine Vorgabe, die die „Argumentationslast“ für die Notwendigkeit der Datenverarbeitung dem Verantwortlichen auferlegt.

Datensicherung

Der Schutz gegen unbefugten Zugriff und unbefugte Veränderung durch Dritte ist Gegenstand der Datensicherung nach Art. 32 DSGVO. Diese obliegt nicht nur dem Verantwortlichen, sondern auch dem Auftragsdatenverarbeiter. Sie umfasst „geeignete technische und organisatorische Maßnahmen“. Welchen Inhalt diese haben sollen, wird mit Hilfe zahlreicher unbestimmter Rechtsbegriffe umschrieben, die ein erhebliches Maß an Unsicherheit bewirken.

Nach Art. 32 Abs. 1 DSGVO müssen bestimmte Umstände berücksichtigt werden. Dazu gehören der „Stand der Technik“, die „Implementationskosten“, „Art, Umfang, Umstände und Zwecke der Verarbeitung“ sowie „Eintrittswahrscheinlichkeit und Schwere des Risikos für

[7] Maas/Schmitz/Wedde, Datenschutz 2014. Probleme und Lösungsmöglichkeiten, 2014,S. 34.

die Rechte und Freiheiten natürlicher Personen.“ Der Verantwortliche oder Auftragsverarbeiter, der sich aller dieser Umstände bewusst sein muss, hat dann durch seine Maßnahmen ein „dem Risiko angemessenes Schutzniveau“ zu gewährleisten. Abs. 1 zählt im Folgenden dann einzelne in Betracht kommende Maßnahmen auf:

(1) Die personenbezogenen Daten können pseudonymisiert oder verschlüsselt werden.
(2) Die Fähigkeit, „die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste“ „im Zusammenhang mit der Verarbeitung“ (warum wohl sonst?) auf Dauer sicherzustellen.
(3) Die Fähigkeit, „die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall“ rasch wiederherzustellen.
(4) „Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“ Wörtlich ins Deutsche übersetzt: Die technischen und organisatorischen Maßnahmen müssen regelmäßig überprüft werden, ob sie weiterhin wirksam die Sicherheit der Verarbeitung gewährleisten. Einfacher könnte es auch heißen: Die technischen und organisatorischen Maßnahmen müssen regelmäßig auf ihre Wirksamkeit hin überprüft werden. Die Sprache der Verordnung macht deutlich, weshalb im Deutschunterricht immer vor einer Häufung von Substantiven gewarnt wurde.

Abs. 2 befasst sich mit dem angemessenen Schutzniveau. Dabei sind „insbesondere“ die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, „insbesondere“ durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung bzw. unbefugten Zugang zu personenbezogenen Daten. Dass gegen Risiken geschützt werden soll, wird niemand bestreiten, auch nicht, dass es bei Daten um die beschriebenen Gefahren geht.

Die vielen Worte vermitteln keine wirkliche Orientierung. Im Grunde geht es darum, unbefugte Zugriffe zu verhindern. Was dafür geeignete Maßnahmen sind, richtet sich nach den konkreten Umständen. Kommt es doch zu einem Zwischenfall, muss dafür gesorgt werden, dass das System möglichst rasch wieder funktioniert. Es wird Aufgabe der Aufsichtsbehörden sein, konkretere Maßstäbe zu entwickeln und die Verantwortlichen sowie die Auftragsverarbeiter zu beraten. Auf diese Weise können die Fortschritte der Informationstechnik besser berücksichtigt werden, als wenn es einen Katalog von feststehenden Maßnahmen geben würde.[8]

[8] Martini, in: Paal/Pauly, Kommentar zur DSGVO, 2017, Art. 32 Rn. 79

Das Problem der IT-Sicherheit