Humanistische Union

Die DSGVO – die wichtigsten Neuerungen aus Sicht der Verbraucher*innen

in: vorgänge Nr. 221/222 (1-2/2018), S. 51-64

*Während die europäische Datenschutz-Grundverordnung die Befugnisse zur Erhebung und Verarbeitung persönlicher Daten für private Stellen (sprich: für Firmen) ausweitet, werden im Gegenzug eine Reihe neuer Rechtsansprüche und Durchsetzungsmöglichkeiten für die Verbraucher*innen geschaffen. Marit Hansen und Sven Polenz stellen die wichtigsten Neuerungen aus Verbrauchersicht dar.*

1. Einleitung

Ab dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung (DSGVO), die für ein einheitliches und gutes Datenschutzniveau in allen europäischen Mitgliedstaaten sorgen soll. Neben der Grundverordnung treten in der nächsten Zeit weitere Neuregelungen in Kraft, z.B. die Datenschutz-Richtlinie für den Bereich Justiz und Inneres, die ebenfalls bis zum 25. Mai 2018 von den Mitgliedstaaten in nationales Recht umgesetzt werden muss und u.a. die Datenverarbeitung der Polizei regelt, oder die für einen etwas späteren Zeitpunkt erwartete ePrivacy-Verordnung, die Datenschutzvorgaben für Telekommunikation und Internet machen wird.[1]

Mit dieser europäischen Datenschutzreform soll das Datenschutzrecht modernisiert und gleichzeitig der starken Zersplitterung der rechtlichen Anforderungen in den Mitgliedstaaten entgegengewirkt werden. Dieses Ziel hatte bereits die EU-Datenschutz-Richtlinie von 1995, doch zum einen sind die Datenverarbeitung und die Risiken von damals mit der heutigen informationstechnisch geprägten Welt nicht vergleichbar, zum anderen haben die Mitgliedstaaten die Vorgaben unterschiedlich interpretiert. Dies – so die Hoffnung des europäischen Gesetzgebers – soll sich nun ändern, denn die DSGVO gilt unmittelbar in allen Mitgliedstaaten. Eigentlich. Denn im mehrjährigen Gesetzgebungsprozess konnte man sich nicht auf alle Details einigen und hat den Mitgliedstaaten in etwa 70 Öffnungsklauseln eigene Regelungsmöglichkeiten eingeräumt, in denen abweichende Interpretationen möglich sind, beispielsweise im Beschäftigtendatenschutz oder bei der Festlegung, ab welchem Alter Jugendliche selbst ihre Einwilligung zu einer Verarbeitung ihrer Daten geben können.

Eine riesige Gesetzesanpassungswelle rollt durch Deutschland, da nicht nur auf Bundesebene, sondern auch in den Bundesländern im Sinne der Rechtsklarheit Hunderte, vielleicht Tausende von Gesetzen, Verordnungen, Erlassen oder Staatsverträgen angepasst werden müssen. Für die Verbraucher*innen in Deutschland besonders wichtig sind aber vor allem zwei Gesetze: die DSGVO selbst und das neue Bundesdatenschutzgesetz (BDSG) mit seinen Regelungen für die Wirtschaft.[2]

Die Grundzüge des Datenschutzrechts bleiben aber dieselben: Personenbezogene Daten dürfen in der Regel nur auf Basis einer Rechtsgrundlage oder einer Einwilligung verarbeitet werden. Die für die Verarbeitung verantwortliche Stelle („der Verantwortliche“) muss im Rahmen ihrer Rechenschaftspflicht nachweisen können, dass sie die DSGVO einhält. Auftragsverarbeiter haben erweiterte Pflichten im Gegensatz zum bisherigen Datenschutzrecht.

Für die Verbraucher*innen – als betroffene Personen – ergeben sich zahlreiche Neuerungen, die im

Folgenden vorgestellt werden.

2. Neue Anforderungen an eine Einwilligung

Die Anforderungen an eine Einwilligung, die Verbraucher*innen erteilen können, waren schon immer anspruchsvoll. Die Grundlage einer wirksamen Einwilligung ist die freie und informierte Entscheidung der betroffenen Person – so die rechtliche Anforderung. Die DSGVO ändert dies nicht und sattelt sogar noch etwas drauf: z.B. dass immer ein Tätigwerden der betroffenen Person nötig ist und aus Stillschweigen keinesfalls auf die Einwilligung geschlossen werden darf (was der Bundesgerichtshof vor Jahren auf Basis des alten BDSG noch anders entschieden hatte) oder dass auf das Widerspruchsrecht explizit hingewiesen werden muss. Die Schriftform wird für die Einwilligung nicht mehr erforderlich sein. Mehr Klarheit soll es online geben, wenn Kinder oder Jugendliche einwilligen. Unschön, dass sich die Mitgliedstaaten nicht auf eine fixe Altersgrenze einigen konnten. Alles zwischen 13 und – so in Deutschland festgelegt – 16 Jahren kann der Mitgliedstaat als Altersgrenze bestimmen, damit nicht zusätzlich die Eltern ihre datenschutzrechtliche Einwilligung für ihren Sohn oder ihre Tochter abgeben müssen. Voraussetzung ist natürlich ein Altersnachweis, wie dies beispielsweise mit dem elektronischen Personalausweis auch online und ohne überschießende Informationen technisch möglich ist.

Im Folgenden wird für die Einwilligung erläutert, was bleibt und was sich ändert:

2.1 Was bleibt unverändert?

Wie bisher in § 4a Abs. 1 BDSG a.F.[3] geregelt, bedarf die Einwilligung für ihre Wirksamkeit einer freien Entscheidung der betroffenen Person. Dies erfordert auch weiterhin, dass die entsprechenden Erklärungen ohne Druck, Täuschung oder Zwang erfolgen. Der betroffenen Person muss eine echte Wahlmöglichkeit zustehen. Ferner muss sie auf den Zweck der Verarbeitung hingewiesen werden. Dies impliziert für Verantwortliche etwa die Verpflichtung, konkret über die Verfolgung von Werbe- oder Marketingzwecken aufzuklären. Unverändert bleibt auch die Pflicht, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben (§ 4a Abs. 1 Satz 4 BDSG a.F.), Die entsprechenden Anforderungen spiegeln sich in der Definition für die Einwilligung in Art. 4 Nr. 11 DSGVO wider. Demnach ist als Einwilligung zu verstehen jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

2.2 Was ist nun zusätzlich zu beachten?

2.2.1 Keine Schriftform erforderlich

Einwilligungen bedürfen zu ihrer Wirksamkeit nicht mehr der Schriftform. Die DSGVO enthält keine dem § 126 BGB vergleichbare Voraussetzung. Nach Erwägungsgrund (ErwGr) 32 Satz 1 DSGVO sind neben schriftlichen auch elektronische oder mündliche Erklärungen ausreichend. Auch an die elektronischen Erklärungen werden keine besonderen Anforderungen geknüpft, insbesondere wird nicht die Verwendung einer qualifizierten elektronischen Signatur gefordert. Erklärungen in Textform sind wirksam. Insbesondere wird nicht die Verwendung einer qualifizierten elektronischen Signatur gefordert. Erforderlich ist nur, dass bei elektronischen Erklärungen die Aufforderung zur Abgabe einer Einwilligung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgt. Unabhängig von der Wirksamkeit mündlicher und elektronischer Erklärungen bleibt der Verantwortliche nach Art. 5 Abs. 2 DSGVO verpflichtet, die Einhaltung der allgemeinen Grundsätze für die Verarbeitung

personenbezogener Daten nachweisen zu können (Rechenschaftspflicht). Von Bedeutung sind hier vor allem die Grundprinzipien einer rechtmäßigen und transparenten Verarbeitung (Art. 5 Abs. 1 a) DSGVO) und der Datenerhebung für festgelegte, eindeutige und legitime Zwecke (Art. 5 Abs. 1 b) DSGVO).

Vor diesem Hintergrund erweist sich die Einholung einer schriftlichen Einwilligung als Vorteil, da der Verantwortliche so die Einhaltung der Anforderungen (Art. 7 und 8 DSGVO) belegen kann. Für elektronische Erklärungen kann der Verantwortliche seinen Pflichten aus Art. 5 Abs. 2 DSGVO u.a. nachkommen, indem er vor allem gewährleistet, dass die betroffene Person ihre Erklärung unter Berücksichtigung der Voraussetzungen nach Art. 7 und 8 DSGVO bewusst und eindeutig abgibt und die Einwilligung protokolliert wird. Bei mündlichen Erklärungen kann zur Erfüllung der Rechenschaftspflicht die Bitte an die betroffene Person um Übersendung einer schriftlichen oder elektronischen Bestätigung der abgegebenen Erklärung ratsam sein.

2.2.2 Verpflichtung auf Opt-in

Einwilligungen können auch in Allgemeinen Geschäftsbedingungen vorformuliert werden. Bisher wurde es dabei als ausreichend betrachtet, dass die betroffene Person eine „Einwilligung“ erklärt, indem sie von der Möglichkeit einer Streichung der Einwilligungsklausel Gebrauch macht oder etwa ein Feld ankreuzt, wonach eine Einwilligung nicht erklärt werde (BGH, Urteil vom 11.11.2009, VIII ZR 12/08). Die Abgabe einer wirksamen Einwilligung muss nach ErwGr 32 DSGVO nun durch eine eindeutige und bestätigende Handlung erfolgen. Stillschweigen, bereits angekreuzte Kästchen oder eine unterstellte Zustimmung, ohne dass die betroffene Person tätig geworden ist, stellen daher keine Einwilligung mehr dar. Erklärungen im Wege eines „Opt-out“ sind nicht mehr zulässig.

2.2.3 Belehrung über ein Widerrufsrecht

Gemäß Art. 7 Abs. 3 DSGVO hat die betroffene Person das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf wird die Rechtmäßigkeit der vorher erfolgten Verarbeitung nicht berührt. Die betroffene Person ist vor der Einwilligung über das Widerrufsrecht und die entsprechende Wirkung eines Widerrufs vom Verantwortlichen in Kenntnis zu setzen. Die bisherigen Einwilligungen nach § 4a BDSG a.F. sind zwar auch widerrufbar. Allerdings fehlte bisher eine entsprechend umfassende Unterrichtungsverpflichtung des Verantwortlichen. Diese Verpflichtung ist ab dem 25. Mai 2018 nun ein zwingender Bestandteil einer jeden Einwilligungserklärung. Jeder betroffenen Person wird damit vor Augen geführt, dass der Bestand ihrer Erklärung von ihrem Willen abhängt.

2.2.4 Anforderungen an die Freiwilligkeit der Einwilligung

Einwilligungen müssen bereits nach § 4a BDSG a.F. auf der freien Entscheidung der betroffenen Person beruhen. Erklärungen, die unter Druck oder Zwang abgegeben werden, sind unwirksam. Nach § 28 Abs. 3b BDSG a.F. darf die verantwortliche Stelle den Abschluss eines Vertrags nicht von einer Einwilligung der betroffenen Person bezüglich der Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung abhängig machen, wenn der betroffenen Person ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam. § 28 Abs. 3b BDSG a.F. soll dabei Sachverhalte erfassen, bei denen der Verantwortliche eine marktbeherrschende Stellung hat, dieser etwa die Preise für Waren oder Dienstleistungen bestimmen kann, und folglich kein gleichwertiger Zugang zu vertraglichen Leistungen anderer Anbieter möglich ist.

Das Kriterium der marktbeherrschenden Stellung des Verantwortlichen sowie die Begrenzung auf Fälle der Werbung und des Adresshandels werden mit der neuen Gesetzeslage aufgegeben. Nach Art. 7 Abs. 4 DSGVO muss künftig bei der Beurteilung der Freiwilligkeit der Einwilligung geprüft werden, ob die Erfüllung eines Vertrags, einschließlich die Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung personenbezogener Daten abhängig gemacht wird, die für die Erfüllung des Vertrags nicht

erforderlich sind.

Beispiel: Ein Verbraucher kauft Schuhe und möchte diese an seinen Wohnsitz liefern lassen. Hierfür benötigt der Verkäufer die Lieferanschrift. Diese ist zur Erfüllung des Vertrags erforderlich. Der Schuhkauf, einschließlich der Lieferung der Schuhe, dürfen aber vom Verkäufer z.B. nicht davon abhängig gemacht werden, dass der Verbraucher ihm die Schuhgröße seiner Ehefrau offenbart. Das letztere Datum ist zur Erfüllung des Vertrags über den Erwerb der Schuhe nicht erforderlich. Der Verbraucher wird davor geschützt, personenbezogene Angaben zu übermitteln, die für die Abwicklung einer vertraglichen Leistung nicht erforderlich sind.

2.2.5 Bedingungen bei Einwilligungen von Kindern

Richten sich Dienste der Informationsgesellschaft (Art. 4 Nr. 25 DSGVO) direkt an Kinder, so ist die auf einer Einwilligung basierende Verarbeitung personenbezogener Daten des Kindes rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Anderenfalls ist die Zustimmung eines Elternteils[4] maßgebend (Art. 8 Abs. 1 DSGVO). Dienste der Informationsgesellschaft sind regelmäßig gegen Entgelt, in elektronischer Form, im Wege des Fernabsatzes erbrachte Dienstleistungen. Es müssen Geräte zum Einsatz kommen, die eine Speicherung der Daten vornehmen, und das Kind muss die Dienstleistung gezielt abrufen können. Sprachtelefonie und die bloße Nutzung eines Fernsehangebots zählen nicht hierzu. Im Kern sind solche Dienste erfasst, die im Internet auf Webseiten für Kinder angeboten werden. Hierbei wird neben dem Inhalt auch die grafische und sprachliche Gestaltung des Angebots den Ausschlag dafür geben, ob sich der Dienst direkt an Kinder richtet. Verbraucher*innen, die das sechzehnte Lebensjahr noch nicht vollendet haben, sollen generell aufgrund fehlender Einsicht und Reife davor bewahrt bleiben, wirksame Einwilligungserklärungen im Internet abzugeben.

3. Änderungen bei den Betroffenenrechten

Verbraucher*innen haben häufig noch nichts davon gehört, dass sie Datenschutzrechte gegenüber den Verarbeitern ihrer personenbezogenen Daten wahrnehmen können. Dabei ist es gar nicht neu, dass jede betroffene Person Auskunft über die zur eigenen Person gespeicherten Daten verlangen, die Berichtigung unrichtiger Daten einfordern oder auf die Löschung von nicht mehr benötigten Daten hinwirken kann. Einen Schritt nach vorn leistet die DSGVO bei den Anforderungen an die Transparenz: Verbraucher*innen sollen künftig mehr Informationen über die Datenverarbeitung erhalten. Schließlich wurde ein ganz neues Recht begründet, dessen langfristige Auswirkungen noch nicht abzuschätzen sind: das Recht auf Datenübertragbarkeit.

Die Betroffenenrechte und ihre Wirkung für die Verbraucher*innen werden im Folgenden erklärt:

3.1 Generelle Anforderungen

Zu den Rechten der Verbraucher*innen nach der DSGVO zählen Informationspflichten bei der Erhebung von personenbezogenen Daten (Art. 13 und 14 DSGVO), das Auskunftsrecht (Art. 15 DSGVO), das Recht auf Berichtigung (Art. 16 DSGVO), das Recht auf Löschung (Art. 17 DSGVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO), die Mitteilungspflicht in Bezug auf die Berichtigung, Löschung oder Einschränkung der Verarbeitung (Art. 19 DSGVO), das Recht auf Datenübertragbarkeit (Art. 20 DSGVO), das Widerspruchsrecht (Art. 21 DSGVO) und das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die der betroffenen Person gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (Art. 22 DSGVO). Die Verantwortlichen müssen den betroffenen Personen die Ausübung ihrer Rechte künftig nach Art. 12 Abs. 2 Satz 1 DSGVO erleichtern. Hierzu zählt etwa, dass

Verbraucher*innen auf ihre Rechte mündlich, schriftlich oder elektronisch hingewiesen werden.

Ferner besteht die Verpflichtung des Verantwortlichen, im Falle der Geltendmachung eines Rechts durch eine Verbraucherin/einen Verbraucher innerhalb eines Monats entsprechende Maßnahmen zu ergreifen und die gestellten Anträge zu erfüllen – also beispielsweise die Anfrage bei einem Verantwortlichen nach allen gespeicherten personenbezogenen Daten im Sinne des Auskunftsrechts. Die Monatsfrist darf unter Berücksichtigung der Komplexität und der Anzahl der Anträge um weitere zwei Monate verlängert werden. In dieser Situation muss der/die Verbraucher*in allerdings eine Zwischennachricht innerhalb des ersten Monats nach Antragseingang erhalten.

3.2 Informationspflichten

Werden personenbezogene Daten bei Verbraucher*innen erhoben, so muss der Verantwortliche diesen zum Zeitpunkt der Datenerhebung eine Reihe von Angaben mitteilen. Gleiches gilt bei Datenerhebungen bei Dritten in Abwesenheit des Verbrauchers, wobei eine nachträgliche Unterrichtung erfolgt. Dazu zählen etwa Angaben zu den Verarbeitungszwecken, zu den Kontaktdaten des Datenschutzbeauftragten, zu den Datenempfängern, zur Speicherdauer, zu den Rechten betroffener Personen nach der DSGVO und zum Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde. Gleiches gilt bei Datenerhebungen bei Dritten in Abwesenheit der Verbraucher*in, wobei eine nachträgliche Unterrichtung erfolgt. Da die Angaben im Zeitpunkt der Datenerhebung vorliegen müssen, können Verantwortliche gehalten sein, z.B. Vertragstexte und Allgemeine Geschäftsbedingungen anzupassen. Im Falle einer Datenerhebung am Telefon wird die Erfüllung der Informationspflichten am Telefon in Betracht kommen. Da mündlich weitergegebene Informationen beim Verbraucher schneller in Vergessenheit geraten können und der Verantwortliche die Einhaltung der Informationspflichten andererseits nachweisen können muss (Art. 5 Abs. 2 DSGVO), ist zu empfehlen, dass für den/die Verbraucher*in die am Telefon mitgeteilten Informationen zusätzlich über elektronische Dienste abrufbar bereitgehalten oder übermittelt werden.

3.3 Auskunftsrecht

Neu ist zugunsten der Verbraucher*innen, dass jede betroffene Person gemäß Art. 15 Abs. 1 DSGVO von dem Verantwortlichen eine Bestätigung darüber verlangen kann, ob sie betreffende personenbezogene Daten verarbeitet werden. Diese Negativauskunft war nach bisherigem Datenschutzrecht nicht vorgesehen und führte in der Praxis zu dem Problem, dass im Einzelfall nicht deutlich wurde, ob der Verantwortliche seiner Auskunftsverpflichtung nicht nachkommt oder er schlicht nicht über Informationen verfügt. Neu ist weiterhin, dass die Auskunftsverpflichtung neben den gespeicherten Daten, den Angaben zu den Empfängern und der Herkunft der Daten nun auch weitere Informationen umfasst, wie etwa Verarbeitungszwecke, geplante Speicherdauer und Hinweise zu Rechten nach der DSGVO. Die betroffene Person muss allerdings in Zukunft damit rechnen, dass ihr nur eine einzige Kopie kostenfrei zusteht. Nach Art. 15 Abs. 3 Satz 2 DSGVO dürfen die Verantwortlichen für jede weitere Kopie ein angemessenes Entgelt verlangen.

3.4 Mitteilungspflicht

Zugunsten der Verbraucher*innen hat der Verantwortliche nach Art. 19 DSGVO künftig die Pflicht, allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung, Löschung oder Einschränkung der Datenverarbeitung mitzuteilen - es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Die Verbraucher*innen haben das Recht, von dem Verantwortlichen eine Unterrichtung über die Empfänger der Daten einzufordern. Mit der Neuregelung ist der Verantwortliche einerseits gehalten, seinen Datenbestand im eigenen Wirkungskreis mit korrekten Angaben zu führen (vgl. Art. 5 Abs. 1d) DSGVO – Grundsatz der Richtigkeit der Daten), wozu auch die Datenverarbeitung durch beauftragte Dienstleister im Wege einer Auftragsverarbeitung (Art. 28 DSGVO) zählt. Andererseits besteht die Verpflichtung, eigene Korrekturen auch Dritten mitzuteilen, um diesen die Führung eines korrekten Datenbestands zu ermöglichen. Hierdurch sollen Nachteile für Verbraucher*innen vermieden werden, die sich stattdessen an jeden Verantwortlichen wenden müssten, um Korrekturwünsche

geltend zu machen. Von Bedeutung kann dies z.B. sein, wenn Verantwortliche an Auskunfteien Angaben übermittelt haben (etwa rechtskräftige Schuldtitel, anerkannte Ansprüche, Informationen zu fälligen und angemahnten Forderungen), die sich nach der Übermittlung als falsch herausgestellt haben. Die Auskunftei wird ihren Datenbestand auf Hinweis des Verantwortlichen aktualisieren und somit dafür sorgen, dass bezüglich der betroffenen Person keine falsche Bonitätsaussage getroffen wird.

3.5 Werbung

Verbraucher*innen müssen vom Verantwortlichen auch weiterhin darüber unterrichtet werden, dass ein Recht besteht, einer Datenverarbeitung für Zwecke der Direktwerbung zu widersprechen. Im Falle eines Widerspruchs ist eine weitere Verarbeitung für Werbezwecke unzulässig (Art. 21 Abs. 2-4 DSGVO). Insoweit bestehen keine wesentlichen Abweichungen gegenüber der bestehenden Rechtslage (vgl. § 28 Abs. 4 BDSG a.F.). Neu für die Verbraucher*innen ist der Umstand, dass das sogenannte Listenprivileg ab dem 25. Mai 2018 entfällt. Der entsprechende in § 28 Abs. 3 BDSG a.F. geregelte Grundsatz räumt den Unternehmen bisher die Möglichkeit ein, einen bestimmten Datensatz (bestehend aus z.B. Namen, Vorname, Titel, Anschrift, Geburtsjahr) für Werbezwecke zu verarbeiten, soweit die Daten aus öffentlich zugänglichen Branchenverzeichnissen stammen oder im Zusammenhang mit einem Vertragsverhältnis rechtmäßig erhoben wurden. Mit der neuen Generalbefugnis zur Rechtmäßigkeit der Datenverarbeitung (Art. 6 Abs. 1 DSGVO) kommt künftig grundsätzlich jedes personenbezogene Datum für Werbezwecke in Betracht. Einschränkungen werden voraussichtlich dort bestehen, wo die Spezialregelungen wie in § 7 Abs. 2 UWG (z.B. Werbung per Telefon und E-Mail) zur Anwendung kommen und damit regelmäßig Einwilligungserklärungen erforderlich sind.

Für die übrigen Werbeformen, für welche keine Spezialbestimmungen eingreifen, ist nach Art. 6 Abs. 1f DSGVO zu prüfen, ob die Verarbeitung des jeweiligen Datums zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Das gilt insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Nach ErwGr 47 DSGVO kann eine Datenverarbeitung für Zwecke der Direktwerbung einem berechtigten Interesse des Verantwortlichen entsprechen. Es zeichnet sich ab, dass besondere Datenkategorien (Art. 9 Abs. 1 DSGVO) wie Gesundheitsdaten, politische Meinungen und Religion regelmäßig nicht für Werbezwecke verarbeitet werden dürfen, da die Interessen der Verbraucher*innen überwiegen werden. Werbung gegenüber Kindern wird selbst mit personenbezogenen Daten, die nicht unter Art. 9 Abs. 1 DSGVO fallen (z.B. Adresse, Angaben zu Hobbys), regelmäßig kaum zulässig sein, da hier vor allem das Kindeswohl und die Einsichtsfähigkeit von Kindern von hoher Bedeutung sind und auch das Vorhandensein eines berechtigten Interesses eines Verantwortlichen zur Datenverarbeitung für die Direktwerbung im Einzelfall argumentativ verneint werden kann.

3.6 Recht auf Datenübertragbarkeit

Art. 20 DSGVO erlaubt es den Verbraucher*innen, die sie betreffenden personenbezogenen Daten vom Verantwortlichen in einem maschinenlesbaren Format zu erhalten. Dahinter steht die Überlegung, dass die betroffenen Personen mit ihren Daten zu anderen Anbietern „umziehen“ können – besonders interessant, wenn (datenschutzfreundlichere) Alternativen zu Quasi-Monopol-Anbietern auf dem Markt auftauchen. Allerdings erwarten einige Beobachter des Marktes einen Effekt, der dem Datenschutzgedanken zuwiderlaufen könnte: Statt ein Mehr an Schutz und Selbstbestimmung zu erreichen, könnten Verbraucher*innen ihre Daten immer dorthin bringen, wo sie den besten monetären Gegenwert erwarten –

also Daten(nutzungs)verkauf statt grundrechtlicher Schutz.

4. Technischer Datenschutz

Die Basis der DSGVO sind die Datenschutz-Grundsätze aus Art. 5 DSGVO, die so umzusetzen sind, dass etwaige Risiken für die Rechte und Freiheiten natürlicher Personen eingedämmt werden. Die Stelle, die für die Datenverarbeitung verantwortlich ist, muss sich der Risiken bewusst sein und angemessene Gegenmaßnahmen treffen. Ein Schwerpunkt dabei besteht im technischen Datenschutz. Dabei geht es jedoch nicht nur um technische und organisatorische Schönheitskorrekturen der Datenverarbeitung, sondern die Gestaltung der Verarbeitung soll von Anfang an darauf ausgerichtet sein, dass die Anforderungen der DSGVO erfüllt werden.[5] Datenschutz soll in die Systeme eingebaut und nicht nachträglich – meistens mit geringerem Wirkungsgrad – aufgepfropft werden. Das soll auch durch Zertifizierungen bestätigt werden können. Außerdem fordert die DSGVO einen professionellen Umgang mit hohen Risiken: In solchen Fällen ist eine Datenschutz-Folgenabschätzung verpflichtend.

Die wichtigsten Auswirkungen für die Verbraucher*innen: Zum einen führen die Anforderungen an Datenschutz und Sicherheit zu einer gesteigerten Vertrauenswürdigkeit der Verarbeitung, wenn der Verantwortliche seine Systeme fortlaufend im Griff hat – d.h. er verfügt über ein funktionierendes Datenschutz- und Informationssicherheitsmanagement. Dann sind auch die personenbezogenen Daten der Verbraucher*innen ausreichend gut geschützt. Zum anderen wird sich die aufgrund der DSGVO zwangsläufig erhöhte Nachfrage für Produkte und Dienstleistungen mit eingebautem Datenschutz auf den Markt auswirken. Auch für Verbraucher*innen werden verbesserte Systeme mit mehr Schutz zur Verfügung stehen. Besonders relevant dabei: Datenschutz als Default-Einstellung.

4.1 Eingebauter Datenschutz und Datenschutz „by Default“

Basis für die Anforderungen des technischen Datenschutzes ist Art. 24 DSGVO, der die Verantwortung regelt. Der darauffolgende Art. 25 regelt Datenschutz durch (Technik-) Gestaltung (Abs. 1) und Datenschutz durch datenschutzfreundliche Voreinstellungen (Abs. 2). Der Verantwortliche muss schon beim Festlegen der Mittel für die Verarbeitung dafür Sorge tragen, dass die rechtlichen Datenschutzanforderungen in geeigneter Weise erfüllt werden. Dies betrifft sämtliche Datenschutz-Grundsätze. Besonders genannt wird die Datenminimierung. Welche technischen und organisatorischen Maßnahmen für den eingebauten Datenschutz geeignet sind, muss der Verantwortliche abwägen. Dabei sind der Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Risiken zu berücksichtigen.

Eine solche Abwägung wird nicht gefordert für die Wahl der Voreinstellungen:[6] Hier besteht die absolute Notwendigkeit, solche Defaults vorzusehen, dass nur die für den jeweiligen Zweck erforderlichen Daten und nur im nötigen Umfang verarbeitet werden. Die Verbraucher*innen müssen aktiv die Konfiguration ändern, damit mehr Daten als erforderlich verarbeitet werden. Hierbei handelt es sich um einen Paradigmenwechsel, denn sehr häufig – beispielsweise in sozialen Netzwerken oder in Apps – sind die Voreinstellungen alles andere als datenschutzfreundlich.

4.2 Datenschutz-Folgenabschätzung

Bei einem voraussichtlich hohen Risiko der Verarbeitung muss der Verantwortliche nach Art. 35 DSGVO eine Datenschutz-Folgenabschätzung durchführen, bevor die Verarbeitung beginnt. Dies ist beispielsweise der Fall bei einer systematischen und umfassenden Bewertung persönlicher Aspekte wie beim Profiling, bei einer umfangreichen Verarbeitung sensibler Daten und bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche. Ziel ist die Beherrschbarkeit des Risikos und Abhilfe durch

geeignete Maßnahmen. Interessant für Verbraucher*innen: Art. 35 Abs. 9 DSGVO sieht vor, dass der Verantwortliche ggf. den Standpunkt der betroffenen Personen oder ihrer Vertreter einholt. Das kann z.B. bedeuten, dass Verbraucherschützer um Stellungnahme gebeten werden.

4.3 Sicherheit und Meldepflichten bei Datenpannen

Auch bei der Informationssicherheit sollen die Verantwortlichen und Auftragsverarbeiter nachlegen. Dies ergibt sich aus Art. 32 DSGVO, wonach geeignete technische und organisatorische Sicherheitsmaßnahmen zu treffen sind. Mindestens genauso motivierend für ein gutes Sicherheitsniveau ist aber die Meldepflicht im Falle von Datenpannen: Nach Art. 33 DSGVO muss der Verantwortliche die Aufsichtsbehörde möglichst binnen 72 Stunden informieren. Wenn aus der Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Verbraucher*innen resultiert, müssen nach Art. 34 DSGVO grundsätzlich auch die betroffenen Personen benachrichtigt werden. Der verlorene USB-Stick mit Kundendaten ist also meldepflichtig – nur dann nicht, wenn ein Risiko faktisch ausgeschlossen werden kann, z.B. wenn es sich um eine Datensicherung handelt, die mit einem Verschlüsselungsverfahren nach Stand der Technik verschlüsselt wurde und ein Finder des USB-Sticks nicht an die Daten herankommen kann.

5. Rechtsbehelfe und Sanktionen

Bislang hatte kaum ein Unternehmen Angst vor möglichen Strafen bei Verstößen gegen das Datenschutzrecht. Zum einen war die Wahrscheinlichkeit, von der Datenschutzaufsichtsbehörde geprüft zu werden, ziemlich klein. Zum anderen waren die Sanktionen, die verhängt werden könnten, vergleichsweise zahnlos, d.h. bestimmt nicht beeindruckend für große Firmen, die ein Bußgeld zur Not aus der Portokasse begleichen konnten.

Die Prüfdichte wird sich auch im neuen Datenschutzregime nicht wesentlich ändern, da die meisten Datenschutzaufsichtsbehörden bislang kaum mehr Prüfpersonal bekommen. Aber innerhalb von drei Monaten nach Eingang einer Beschwerde müssen die Behörden aktiv geworden sein – sonst laufen sie Gefahr, verklagt zu werden. Neu sind auch mögliche Schadensersatzansprüche von betroffenen Personen und der stark erweiterte, recht eindrucksvolle Bußgeldrahmen, selbst wenn nicht ständig die Maximalhöhe an Bußgeldern verhängt werden wird.

5.1 Rechtsbehelfe

Betroffene Personen können nach Maßgabe von Art. 77 Abs. 1 DSGVO im EU-Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes Beschwerde bei einer Aufsichtsbehörde einlegen. Die kontaktierte Aufsichtsbehörde wird die betroffene Person über den Stand des Beschwerdeverfahrens oder gegebenenfalls über das Ergebnis dieses Verfahrens unterrichten. Betroffene Personen können nach Art. 78 Abs. 2 DSGVO einen gerichtlichen Rechtsbehelf gegenüber einer zuständigen[7] Aufsichtsbehörde im Zusammenhang mit einem Beschwerdeverfahren geltend machen, wenn innerhalb von drei Monaten keine Befassung mit der Beschwerde erfolgte. Weiterhin besteht ein gerichtlicher Rechtsbehelf auch dann gegenüber einer Aufsichtsbehörde, wenn diese den Beschwerdeführer nicht innerhalb von drei Monaten zum Stand des Beschwerdeverfahrens oder gegebenenfalls zu den Prüfergebnissen unterrichtet. Betroffene Personen haben darüber hinaus das Recht, eine Klage gegen Verantwortliche oder Auftragsverarbeiter wegen der Verletzung von Vorgaben der DSGVO zu erheben. Nach Art. 79 Abs. 2 DSGVO sind in diesem Fall die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder Auftragsverarbeiter eine Niederlassung hat. Wahlweise wäre auch eine Klageerhebung am Ort des Aufenthaltsorts der betroffenen Person zulässig, soweit es sich bei der Klagegegnerin nicht um

die Behörde eines anderen Mitgliedstaats handelt.

5.2 Schadensersatz

Entsteht den Verbraucher*innen aufgrund der Verletzung von Vorgaben der DSGVO ein materieller oder immaterieller Schaden, so kommt ein Schadensersatzanspruch gegen den Verantwortlichen oder Auftragsverarbeiter in Betracht. Auftragsverarbeiter haften nur dann für einen verursachten Schaden, wenn diese ihre spezifischen Pflichten aus dem Auftragsverhältnis verletzen (vgl. vor allem Art. 28 Abs. 2, 3 und 10 DSGVO) oder einer rechtmäßig erteilten Weisung des Auftraggebers (vgl. Art. 29 DSGVO) zuwiderhandeln. Dem Verantwortlichen und dem Auftragsverarbeiter obliegen die Beweislast dafür, dass sie für einen eingetretenen Schaden nicht verantwortlich sind. Eine Besonderheit ist künftig auch die gesamtschuldnerische Haftung von Verantwortlichem und Auftragsverarbeiter nach Art. 82 Abs. 4 DSGVO. Die Zuständigkeit der Gerichte in den Mitgliedstaaten für Klagen, mit denen ein Schadensersatzanspruch verfolgt wird, richtet sich nach Art. 79 Abs. 2 DSGVO und damit nach dem Sitz der Niederlassung des Klagegegners oder wahlweise nach dem Ort des Aufenthalts der betroffenen Person, mit Ausnahme von Klagen gegen eine Behörde im letzteren Fall.

5.3 Bußgelder

Die Aufsichtsbehörden haben nach Art. 58 Abs. 2i DSGVO die Befugnis, bei Verstößen gegen die Vorgaben der DSGVO Geldbußen zu verhängen. Der europäische Verordnungsgeber hat dafür hohe Bußgeldrahmen vorgesehen, die Geldbußen von bis zu 10 bzw. 20 Millionen Euro oder im Falle eines Unternehmens von bis zu 2 bzw. 4 Prozent seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres umfassen können. Die Mitgliedstaaten können nach Art. 83 Abs. 7 DSGVO für ihren Hoheitsbereich Vorschriften festlegen, ob und in welchem Umfang gegen Behörden und andere öffentliche Stellen Geldbußen verhängt werden können. Nach derzeitigem Kenntnisstand ist für die laufenden Gesetzgebungsverfahren in den Bundesländern nicht zu erwarten, dass von dieser Gesetzgebungsbefugnis Gebrauch gemacht wird – es bleibt also dabei, dass Datenschutzbehörden gegenüber öffentlichen Stellen in Deutschland keine Bußgelder verhängen können. Im Zusammenhang mit Auskunftsverlangen von Darlehensgebern bei Verbraucherkrediten kommt ein neuer Bußgeldtatbestand nach nationalem Recht hinzu (vgl. § 30 BDSG n.F. – BGBl. I, Nr. 44 v. 5.7.2017).

6. Instrumenten-Mix neben der Datenschutzaufsicht

Neben den Datenschutzaufsichtsbehörden werden weiterhin die Verbraucherzentralen eine wichtige Rolle im Sinne der Datenschutz-Compliance spielen. Außerdem können Vereine die Verbraucher*innen in ihren Rechten unterstützen:

Wer Vorschriften zuwiderhandelt, die dem Schutz der Verbraucher*innen dienen, kann im Interesse des Verbraucherschutzes nach § 2 Abs. 1 Satz 1 des Unterlassungsklagengesetzes (UklaG) auf Unterlassung und Beseitigung in Anspruch genommen werden. Die Verbraucherzentralen prüfen in diesem Kontext nach § 2 Abs. 2 Nr. 11 UKlaG auch Vorschriften, welche die Zulässigkeit der Datenerhebung von Verbraucher*innen durch ein Unternehmen bzw. der Verarbeitung oder der Nutzung personenbezogener Daten, die von Unternehmen über Verbraucher*innen erhoben wurden, betreffen. Das können Fälle sein, in denen die Daten zu Zwecken der Werbung, Markt- und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben, verarbeitet oder genutzt werden. Um der Gefahr einer divergierenden Beurteilung von Datenschutzverstößen durch die Verbraucherzentralen und die Aufsichtsbehörden zu begegnen, sind die Gerichte (wie bisher auch) angehalten, vor ihrer Entscheidung in Verfahren über einen Anspruch nach § 2 UKlaG die zuständige inländische Datenschutzaufsichtsbehörde

anzuhören.

Die Verbraucher*innen können sich zudem durch Nicht-Regierungs-Organisationen wie den jüngst gegründeten Verein noyb[8] helfen lassen. Diesem und ähnlich ausgerichteten Vereinen geht es darum, den Klageweg für eine effektivere Durchsetzung des neuen EU-Datenschutzrechts zu nutzen und mit strategischen Klagen die Rechte und Freiheiten der Bürger*innen zu stärken. Diese Herangehensweise basiert auf Art. 80 DSGVO, nach dem solche Organisationen im Namen von betroffenen Personen die Beschwerde einreichen oder auch das Recht auf Schadensersatz gemäß Art. 82 in Anspruch nehmen können.

Die nächsten Jahre werden geprägt sein von Aushandlungsprozessen, wie die einzelnen Regelungen in der Praxis europaweit möglichst einheitlich zu interpretieren sind. Im optimalen Fall wird ein Wetteifern über den besseren Datenschutz und die cleversten Lösungen zum Schutz der Rechte und Freiheiten entstehen. Risiken werden eingedämmt, jeder ist sich seiner Verantwortung bewusst, Missstände werden sanktioniert und abgestellt. Und wenn die DSGVO keinen Fortschritt im Datenschutz bringen sollte? Die DSGVO ist nicht statisch, sondern sieht einen Anpassungsmechanismus vor. Nach Art. 97 DSGVO steht die erste Evaluation bis zum 25. Mai 2020 an. Bis dahin sollte Klarheit bestehen, wo Verbesserungen notwendig sind.

MARIT HANSEN Jahrgang 1969, Dipl.-Inform., seit 2015 Landesbeauftragte für Datenschutz Schleswig-Holstein und Leiterin des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, seit 1995 beruflich im Datenschutz tätig. Ihr Schwerpunkt liegt auf der Gestaltung von Systemen im Sinne des Datenschutzes „by Design & by Default“.

SVEN POLENZ Jahrgang 1976, Dr. iur., LL.M., Referatsleiter für die Bereiche Datenschutz in der Privatwirtschaft und Informationsfreiheit am Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein. Jüngste Veröffentlichung: Brink/Polenz/Blatt, Informationsfreiheitsgesetz (Kommentar), C.H. Beck 2017.

Anmerkungen:

1 S. dazu die Beiträge von Aden und Glatzner in diesem Heft.

2 S. dazu die Beiträge von Weichert und Schaar in diesem Heft.

3 Das bisherige BDSG wird in diesem Beitrag mit „BDSG a.F.“ bezeichnet, das ab dem 25.05.2018 geltende BDSG mit „BDSG n.F.“.

4 Um ganz präzise zu sein: die Zustimmung der Träger des elterlichen Sorgerechts.

5 Zur Reichweite des Risikobegriffs nach der DSGVO vgl. den Beitrag von Rost in diesem Heft.

6 Wer aus dem Wort „grundsätzlich“ in Art. 25 Abs. 2 S. 1 DSGVO schließt, dass Ausnahmen vorgesehen sind, sei auf die englische Sprachfassung verwiesen – es handelt sich im Deutschen um einen Übersetzungsfehler.

7 Dies ist der Fall, sofern die Aufsichtsbehörde in ihrem eigenen Hoheitsbereich bzw. Mitgliedstaat tätig werden kann (Art. 55 DSGVO) bzw. es sich um eine federführende Aufsichtsbehörde i.S.v. Art. 56 DSGVO handelt.

8 Der Verein wurde von dem Datenschutz-Aktivisten Max Schrems gegründet. Der Namen steht für „none of your business“, s. https://www.noyb.eu/.

---

https://www.humanistische-union.de/publikationen/vorgaenge/221-222/publikation/die-dsgvo-die-wichtigsten-neuerungen-aus-sicht-der-verbraucherinnen/

Abgerufen am: 23.04.2024