Diese Erörterung gehört zum WebBaecker Infodienst 26/2018 - www.webbaecker.de - erschienen am 29.06.2018

Die neuen datenschutzrechtlichen Regelungen der EU-Datenschutzgrundverordnung und im neuen Bundesdatenschutzgesetz

RA Tom-Christian Uhland, Gehrke Econ Rechtsanwaltsgesellschaft mbH

Am 25. Mai 2018 ist die EU-Datenschutz-Grundverordnung (DSGVO) in Kraft getreten. Gleichzeitig mit der DSGVO trat die Neufassung des Bundesdatenschutzgesetzes (BDSG) in Kraft.

Die DSGVO soll das Datenschutzrecht EU-weit vereinheitlichen. Nach der DSGVO ist die Datenverarbeitung weiterhin nur zulässig, wenn es die Verordnung oder ein anderes Gesetz ausdrücklich erlaubt (sog. Verbot mit Erlaubnisvorbehalt), vgl. Art. 6 Abs. 1 DSGVO. Dies galt auch schon nach dem bisherigen BDSG, insofern gibt es hier keine gravierenden Änderungen. Erforderlich für die Datenverarbeitung ist daher entweder eine Einwilligung des Betroffenen oder ein Rechtfertigungsgrund nach Art. 6 Abs. 1 DSGVO, etwa wenn die Datenverarbeitung zur Erfüllung eines Vertrages erforderlich ist, was in der Praxis der häufigste Fall einer erlaubten Datenverarbeitung darstellt.

Nach einer zweijährigen Übergangsfrist müssen ab dem 25.05.2018 alle Dokumente und Prozesse an die neuen Vorschriften der DSGVO angepasst sein. Problematisch ist, dass die DSGVO im Vergleich zum neuen Bundesdatenschutzgesetz (BDSG) einige Änderungen vorsieht. Allerdings gilt das neue BDSG auch mit Inkrafttreten der DSGVO weiter - es sind also beide Regelwerke zu beachten! Dabei hat die DSGVO Vorrang vor dem BDSG, soweit diese keine ausdrücklichen Möglichkeiten für eine einzelstaatliche Regelung vorsieht.

In der Vergangenheit wurde die Einhaltung des Datenschutzes vielfach nicht so genau genommen. Nunmehr sieht die DSGVO zukünftig erhebliche Bußgelder bei datenschutzrechtlichen Verstößen vor, die gemäß Art. 83 Abs. 5 DSGVO bis zu vier Prozent des Umsatzes betragen können. Weitgehend jede neue Vorgabe ist bußgeldbewehrt. Unternehmen sind daher gut beraten, fachkundige Beratung in Anspruch zu nehmen, um die gebotenen technischen und organisatorischen Änderungen zu ergreifen. Der nachfolgende Artikel soll einen kurzen Überblick auf die aus Sicht des Verfassers wichtigsten Änderungen geben.

I. Grundlagen und Begrifflichkeiten

1. Personenbezogene Daten

Personenbezogene Daten sind gem. Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wobei auch eine mittelbare Möglichkeit der Identifikation, etwa über das Geburtsdatum und die Adresse ausreicht. Damit sind personenbezogene Daten alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (dem „Betroffenen“) wie: Alter, Geschlecht, Anschrift, Religion, sexuelle Orientierung, Vermögen, Äußerungen, politische und weltanschauliche Überzeugungen usw.

2. Anwendungsbereich

Die Datenschutzgrundverordnung greift ein, wenn personenbezogene Daten verarbeitet werden. Nun könnte man meinen, dass hiervon nur die computergestützte Datenverarbeitung betroffen ist. Diese Annahme ist weit verfehlt. Erfasst ist gemäß Art. 2 Abs. 1 DSGVO schon die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert werden sollen. Damit sind Akten, die nach personenbezogenen Kriterien geführt werden, etwa Kundenakten, von dem sachlichen Anwendungsbereich der Datenschutzgrundverordnung betroffen. Die DSGVO gilt gem. Art. 2 DSGVO für die ganze oder teilweise automatisierte Datenverarbeitung personenbezogener Daten sowie für die nichtautomatisierte Datenverarbeitung personenbezogener Daten, die in einem Dateispeichersystem gespeichert sind oder werden sollen. Damit ist die DSGVO anzuwenden, wenn Daten:

- unter Einsatz von Datenverarbeitungsanlagen (z. B. Computer, Diktiergerät) oder
- nicht automatisiert (z. B. Erfassung auf einem Blatt Papier mit Stift) und dann in einem Dateisystem (= strukturierte Sammlung etwa nach Jahr, Aktenzeichen oder Namen in alphabetischer Reihenfolge) gespeichert werden sollen.

Damit ist der Anwendungsbereich der DSGVO weit gefasst, sie betrifft jedes Unternehmen.

Hinweis:

Ausgenommen sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für ausschließlich persönliche oder familiäre Zwecke und Tätigkeiten.

3. Verbot mit Erlaubnisvorbehalt, Einwilligung, Newsletterversand

a) Grundsatz: Verbot mit Erlaubnisvorbehalt

Die Verarbeitung personenbezogener Daten unterliegt gemäß Art. 6 DSGVO einem Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass jede Datenverarbeitung verboten ist, die nicht **gesetzlich erlaubt** oder in die der Betroffene **nicht eingewilligt** hat.

Die Erlaubnistatbestände sind in Art. 6 DSGVO geregelt. Danach ist die Verarbeitung nur dann rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur **Durchführung vorvertraglicher Maßnahmen** erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;
- die Verarbeitung ist erforderlich, um **lebenswichtige Interessen der betroffenen Person** oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung ist für die **Wahrnehmung einer Aufgabe** erforderlich, die **im öffentlichen Interesse** liegt oder **in Ausübung öffentlicher Gewalt** erfolgt, die dem Verantwortlichen übertragen wurde;
- die Verarbeitung ist zur **Wahrung der berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

b) Die Einwilligung nach DSGVO

Soll eine Einwilligung des Betroffenen Grundlage für eine Erhebung, Verarbeitung oder Nutzung sein, muss diese gemäß Art. 7 DSGVO

- freiwillig erfolgen,
- die Einwilligung muss in transparenter Weise eingeholt werden (d. h. nicht im Kleingedrucktem versteckt und deutlich hervorgehoben)
- mit Erklärungsbewusstsein abgegeben (vgl. Art. 4 Nr. 1 DSGVO) werden: Keine im Vorhinein angekreuzten Kästchen oder im Vertragswerk versteckte Einwilligungserklärungen mehr. Auch kann keine Einwilligung mehr unterstellt werden, wenn der Vertragspartner der Datenverarbeitung nicht widerspricht (sog. opt-out Lösung)
- die Einwilligung muss nachgewiesen werden können
- Bestimmtheit der Einwilligung: Diese muss sich auf einen bestimmten Zweck (z. B. Newsletter) beziehen, keine Generaleinwilligung möglich.
- Einsichtsfähigkeit, Art. 8 DSGVO: Der Betroffene muss mindestens 16 Jahre alt sein.

Die Einwilligung bedarf **nicht zwingend der Schriftform**, sondern diese kann auch **in protokollierter elektronischer Form** eingeholt werden. In diesem Falle müssen die obigen Voraussetzungen erfüllt sein und die Einwilligung muss gemäß Art. 32 EGDSGVO in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes abgegeben werden.

Häufiges Problem in der Praxis kann die „Freiwilligkeit" der Einwilligung sein. Diese wird etwa im Arbeitsverhältnis in Frage gestellt, da hier der Arbeitnehmer aufgrund seiner Stellung keine andere Wahl hat, als einzuwilligen. Aufgrund dieser Zwangslage sollen Einwilligungen in überwachende Maßnahmen unwirksam sein. Glücklicherweise regelt das neue BDSG in § 26 BDSG, dass die Datenverarbeitung im Arbeitsverhältnis grundsätzlich dann erlaubt ist, wenn die Daten für die Durchführung oder Beendigung des Arbeitsverhältnisses benötigt werden.

4. Newsletterversand; Veranstaltungen

Gerade beratende Unternehmen und Unternehmen des Versandhandels setzen zur Information ihrer Kunden Newsletter ein oder laden Kunden und Mandanten zu Vortragsveranstaltungen ein. Da auch hier noch kein Datenverarbeitung rechtfertigender Vertrag geschlossen wurde, muss für die Datenverarbeitung für diese **werblichen Zwecke eine Einwilligung des Adressaten** vorliegen. In der Vergangenheit waren diese Einwilligungen nicht mit der hinreichenden Deutlichkeit und Transparenz abgefordert worden, weshalb diese häufig noch einmal eingeholt werden müssen.

II. Die Prinzipien der DSGVO

Die Zentralnorm von Art 5 DSGVO listet folgende Grundprinzipien auf, die zukünftig von Unternehmen bei der Datenverarbeitung zu beachten sind:

- Einhaltung der **Datenschutzgrundsätze** (Art. 5 Abs. 1, 2 DS-GVO): Datenminimierung, Richtigkeit Speicherbegrenzung, Integrität und Vertraulichkeit
- Rechenschaftspflicht
- **Rechtmäßigkeit** der Datenverarbeitung (Verbot mit Erlaubnisvorbehalt)
- Treu und Glauben (Verhältnismäßigkeit)
- **Transparenz** bei der Erhebung durch angemessene Information der Betroffenen, Art. 12 ff. DS-GVO

- **Zweckbindung** der Datenverarbeitung
- **Sicherheit** der Verarbeitung durch Umsetzung geeigneter technischer und organisatorischer Maßnahmen (Art. 24, 32 DS-GVO)
- **Datenschutzkonforme Auftragsverarbeitung**
- **Dokumentation der Verarbeitungstätigkeiten**

Gerade die Rechenschaftspflicht führt zu erheblichen Dokumentations- und Nachweispflichten in der Praxis, da der Nachweis der Erfüllung der Anforderungen der DSGVO nachgewiesen werden können muss. Dies erfordert eine umfangreiche Dokumentation der datenverarbeitenden Prozess und der getroffenen Maßnahmen.

III. Die Rechte der Betroffenen

Die DSGVO regelt explizit die Rechte der von der Datenverarbeitung betroffenen Personen. Insbesondere stehen diesen Personen folgende Rechte zu:

- **Auskunftsrecht** gemäß Art. 15 DSGVO über die verarbeiteten personenbezogenen Daten
- **Berichtigungsrecht** gemäß Art. 16 DSGVO bzgl. unrichtiger oder Vervollständigung der gespeicherten personenbezogenen Daten;
- **Löschungsrecht** gemäß Art. 17 DSGVO, soweit die Daten nicht die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, aus Gründen des öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist;
- **Einschränkung der Verarbeitung** gemäß Art. 18 DSGVO
- **Widerspruchsrecht** gemäß Art. 21 DSGVO
- **Recht auf Übertragbarkeit** gemäß Art. 20 DSGVO
- **Jederzeitige Widerruflichkeit der Einwilligung** gemäß Art. 7 Abs. 3 DSGVO
- **Beschwerderecht bei Aufsichtsbehörde** gemäß Art. 77 DSGVO

Über diese Rechte ist der Betroffene gemäß Art. 13 Abs. 2, 14 Abs. 2 DSGVO bei der Datenerhebung zu informieren.

IV. Informationspflichten nach Art. 13, 14 DSGVO, insbesondere Datenschutzerklärung auf der Homepage

Ein wesentliches Anliegen der Datenschutzreform ist die Stärkung des sog. Transparenzprinzips, d. h. die von der Datenerhebung betroffenen Personen sollen besser über die Datenverarbeitung selbst und die bestehenden Rechte informiert werden. Aufgrund dessen müssen die betroffenen Personen in transparenter und verständlicher Weise insbesondere über die datenverarbeitende Stelle, Art und Umfang der Datenverarbeitung, die bestehenden Rechte sowie über die Rechtsgrundlage der Datenverarbeitung informiert werden, sobald personenbezogene Daten „erhoben“ werden. Personenbezogene Daten sind alle Informationen mit denen eine Person unmittelbar (z. B. Name) oder mittelbar identifiziert werden kann (z. B. über eine Adresse). Die Verordnung differenziert danach, ob die Daten unmittelbar beim Betroffenen (vgl. Art. 13 DSGVO) oder nicht direkt bei dem Betroffenen (Art. 14 DSGVO), erhoben werden. In der Praxis am relevantesten für Unternehmen ist die Direkterhebung, weshalb im Folgenden nur auf die Informationspflichten für die Direkterhebung von Daten beim Kunden eingegangen werden soll.

1. Zeitpunkt der Informationen

Die Informationspflichten knüpfen an den „Zeitpunkt der Erhebung“ an. Dies ist der Zeitpunkt, zu dem auf die Daten erstmalig zugegriffen werden soll. Umstritten ist dabei, welcher Zeitpunkt hiermit gemeint ist. Die schärfste Meinung knüpft daran an, dass die Informationspflichten unmittelbar vor Beginn der Datenerhebung erfüllt

werden müssen[1]. Denn nach dieser Auffassung sollen die Informationspflichten ermöglichen, dass der Betroffene darüber entscheiden kann, ob er in die Datenverarbeitung einwilligt oder hiergegen Einwände erhebt.

Ausreichend ist, wenn die Daten auf einem Formular erhoben werden, auf dem sich die gebotenen Informationen befinden. So könnten die Informationen etwa auf einem Registrierungsformular auf einer Webseite enthalten oder als Anhang an ein auszufüllendes Vertragsformular beigefügt bzw. deutlich sichtbar dort wiedergegeben werden.

2. Sonderfall Homepage

Die DS-GVO stellt besondere Anforderungen an die Betreiber einer Homepage, so dass die Datenschutzerklärungen in der Regel überarbeitet und besondere Hinweise schon bei dem Besuch einer Homepage gegeben werden müssen, etwa wenn durch die Verwendung von Cookies Daten der Besucher wie die IP-Adresse verarbeitet werden. Regelmäßig wird beim Besuch einer Homepage die sogenannte IP-Adresse des Besuchers erfasst, mit derer der Betroffene identifiziert werden könnte. Damit aber sind die Informationspflichten schon beim Besuch der Homepage zu erfüllen, in der Praxis wird hierzu eine Datenschutzerklärung verwendet, in welcher die nach Art. 13 DSGVO erforderlichen Informationen wiedergegeben sind. Nähere Informationen über die neuen Anforderungen für Betreiber von Webseiten könne über die Homepage des Landesbeauftragten für den Datenschutz unter folgenden Link abgerufen werden:

http://www.lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/informationen_betreiber_von_webseiten/informationen-fuer-betreiber-von-webseiten-zur-anpassung-an-die-vorgaben-der-datenschutz-grundverordnung-ab-dem-25052018-164589.html .

3. Sonderfall Cookies und Social Media Plug-Ins

a) Cookies

Nahezu alle Webseiten verwenden Cookies. Diese sind dazu da, Nutzer wiederzuerkennen und das Surfen auf einer Website zu erleichtern, etwa dadurch dass der Nutzer seine Zugangsdaten nicht bei jedem Besuch neu eingeben muss oder erkannt wird, was der Nutzer bereits gekauft hat. Dabei handelt es sich um kleine Dateien, die vom Browser automatisch erstellt und die auf dem Endgerät (Laptop, Tablet, Smartphone o. ä.) des Betroffenen gespeichert werden, wenn eine Homepage besucht wird.

Nach dem aktuellen Positionspapier der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. April 2018 bedarf der Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und etwa der Erstellung von Nutzerprofilen dienen, jedenfalls einer **vorherigen Einwilligung**. Das bedeutet, dass eine informierte Einwilligung i. S. d. DSGVO, in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung vor der Datenverarbeitung eingeholt werden muss, d. h. z. B. bevor Cookies platziert werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.

b) Social Media-Plug-Ins

Sogenannte Social Media-Plug-Ins werden von den großen Social Media-Plattformen wie Facebook, Google+, Twitter oder Pinterest zur Verfügung gestellt, etwa in Form eines „Gefällt mir"-Buttons.

Diese Plug-Ins werden von Betreibern von Webseiten auf ihren Seiten eingebaut und sollen den Besuchern ermöglichen, Blogseiten oder Produkte einfach ihren Kontakten über die jeweilige Social Media Plattform zu empfehlen. Webseitenbetreiber erhoffen sich dadurch meist Umsatzsteigerungen, insbesondere da persönliche Empfehlungen eine deutlich größere Wirkung haben können als etwa ein Werbebanner.

---

1 Vgl. Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, Art. 13 DS-GVO Rn. 56 mit dem Streitstand.

Facebook erhält generell bei jedem Aufruf eines in einer Webseite eingebundenen Like-Buttons, unabhängig davon, ob der Webseitenbesucher ein Facebook-Nutzer ist oder nicht, die „Grunddaten" eines Webseitenaufrufs: IP-Adresse, Uhrzeit und Datum des Webseitenaufrufs, Internetadresse, über die das Facebook Social Plug-In aufgerufen wurde sowie browserspezifische Informationen (beispielsweise welcher Browser verwendet wurde). Da dabei personenbezogene Daten übertragen werden, sind in gleicher Weise Informationspflichten zu erfüllen. Dies erfolgt auch regelmäßig in einer Datenschutzerklärung.

Problematisch bei der Verwendung von Social Media Plug-Ins ist, dass vor Betätigung des Buttons keine Einwilligung eingeholt wird. Eine solche ist aber erforderlich, da diese Plug-Ins nicht durch einen erlaubten Zweck, etwa zur Vertragserfüllung verwendet werden, sondern lediglich der Werbung und Umsatzsteigerung dienen. Damit aber bedarf die Verwendung solcher Plug-Ins der **vorherigen Einwilligung** nach Art. 7 DSGVO.

Daher müssen die Betroffenen **zukünftig vor der Verwendung des Plug-Ins aufgeklärt und eine Einwilligung eingeholt** werden. Der Nutzer muss eine explizite Erklärung bestätigen (z. B. durch Anklicken/Anhaken eines Kästchens) oder durch eine andere eindeutige bestätigende Handlung (z. B. die Vorauswahl von Browser-Einstellungen). Die Einwilligung muss stets nachgewiesen werden können.

4. Inhalt und Form der Informationspflichten gemäß Art. 13, 14 DSGVO

Inhalt und Form der Informationspflichten sind in Art. 13, 14 DSGVO geregelt. Hierbei ist zwischen den Pflichtinformationen (Art. 13 Abs. 1 und Art. 14 Abs. 1 DSGVO) und den Informationen zu unterscheiden, die nur dann mitgeteilt werden müssen, wenn diese für eine faire und transparente Verarbeitung der Daten erforderlich sind (Art. 13 Abs. 2 und Art. 14 Abs. 2 DSGVO). Da viele der in den Art. 13 Abs. 2 und Art. 14 Abs. 2 DSGVO genannten Informationen für einen Betroffenen wesentlich sind, sollten diesem rein vorsorglich alle Informationen zur Verfügung gestellt werden, die Art. 13, 14 DSGVO auflistet.

Im Einzelnen sollte die Datenschutzerklärung bzw. das Informationsblatt folgende Informationen beinhalten:

- Kontaktdaten des verantwortlichen Unternehmens und des Vertreters
- Benennung des Datenschutzbeauftragten nebst Kontaktadresse
- Zweck der Datenverarbeitung
- Rechtsgrundlage der Datenverarbeitung
- Angabe der berechtigten Interessen, welche die Datenverarbeitung rechtfertigen, sofern diese auf den Erlaubnistatbestand von Art. 6 Abs. 1 DSGVO gestützt wird.
- Angabe der Empfänger der erhobenen Daten
- Information, ob die Daten bei der Verarbeitung auch an Server weitergeleitet werden, die sich außerhalb der EU befinden und ob in diesen Fällen mit den jeweiligen Ländern entsprechende Datenschutzabkommen bestehen, mit denen ein ähnliches Schutzniveau wie innerhalb der EU gewährleistet werden soll (z.B. Privacy Shield Abkommen mit den USA)
- Dauer der Datenspeicherung (Speicherfristen)
- Information über die Rechte der Betroffenen (z. B. Auskunftsrecht, Löschungsrecht, Widerruflichkeit der Einwilligung, Einschränkung der Datenverarbeitung, Widerspruchsrecht, Beschwerderecht des Betroffenen bei der Datenschutzbehörde, Hinweis auf das Recht zur Datenübertragbarkeit)
- Ob die Bereitstellung der personenbezogenen Daten gesetzlich (z. B. Geldwäsche) oder für einen Vertragsabschluss erforderlich ist
- Das Bestehen einer automatisierten Entscheidungsfindung inkl. Profiling

Der Link zu den Informationspflichten, die typischer Weise in einer Datenschutzerklärung enthalten sind, sollte ähnlich wie das Impressum einfach möglichst direkt über die Startseite der Website erreichbar sein. Der Text muss in Deutsch und bei internationaler Ausrichtung des Angebots auch in weiteren Sprachen verfasst sein.

Aber auch ohne Internetauftritt besteht eine Informationspflicht nach Art. 13 DSGVO. Regelmäßig wird etwa bei Lieferungen an Kunden mindestens deren Name und Adresse sowie die Telefonnummer erfasst, die dann häufig

in einer Kundenkartei aufgenommen werden. So ist etwa derjenige Bäcker oder Fleischer, der einen Partyservice betreibt, grundsätzlich verpflichtet, dem Kunden ein Informationsblatt zum Zeitpunkt der Erhebung der Daten zur Verfügung zu stellen.

V. Datensicherheit, Art. 32 DSGVO

Zukünftig sind Verstöße gegen die Datensicherheit mit einer Strafe von bis zu zwei Prozent des Umsatzes bußgeldbewehrt. Art. 32 DSGVO regelt die Vorgaben für die Datensicherheit.

Die Prozesse zur Umsetzung der Gewährleistung der Datensicherheit sind in folgenden Schritten umzusetzen:

- Risikoanalyse: Welche Risiken bestehen durch Vernichtung, Verlust, Veränderung oder unbefugtem Zugang Dritter?
- Risikobewertung: Wie hoch und schwer ist das Risiko?
- Ergreifung geeigneter technischer und organisatorischer Maßnahmen

Danach müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Als Beispiel für entsprechende Maßnahmen nennt die Vorschrift folgende Maßnahmen

a) die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;

b) die Fähigkeit, die **Vertraulichkeit**, **Integrität**, **Verfügbarkeit und Belastbarkeit der Systeme** und Dienste im Zusammenhang mit der Verarbeitung auf Dauer **sicherzustellen**;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch **wiederherzustellen**;

d) ein Verfahren zur **regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen** zur Gewährleistung der Sicherheit der Verarbeitung.

In Konsequenz sollte daher zukünftig der E-Mail-Verkehr und der Verkehr über die Internetseite verschlüsselt werden. Zudem müssen Datensicherungs- und Berechtigungskonzepte entwickelt werden. Flankierend treffen die Vorschriften der Art. 24, 25 DSGVO weitere Regelungen zur Sicherstellung eines angemessenen Schutzniveaus, auf die hier aber nur kurz eingegangen werden kann.

VI. Ergreifung geeigneter technischer und organisatorischer Maßnahmen (TOM)

Der Schutz personenbezogener Daten erhält durch die DSGVO einen noch höheren Stellenwert als es im BDSG der Fall war. Die DSGVO stellt daher hohe Anforderungen an die Technik und die interne Organisation des verantwortlichen Unternehmers, da Datensicherheit zu gewährleisten ist. Verantwortliche müssen nach Art. 24, 25 DSGVO geeignete technische und organisatorische Maßnahmen (TOM) treffen. Hierzu ist eine umfangreiche Bestandsanalyse vorzunehmen und ein Datenschutz-Management-System einzuführen. Die DSGVO beschreibt, dass bei der Auswahl der Sicherheitsmaßnahmen der Stand der Technik und die Implementierungskosten zu berücksichtigen sind. Daraus ergibt sich, dass gerade im IT-Sicherheitsumfeld Budget vorhanden sein muss, um geeignete Soft- und Hardware beschaffen und einsetzen zu können.

Bei der Sicherheit der Verarbeitung geht es nicht nur darum, böswillige Attacken von außen abzuwehren, sondern auch den Risiken mit Sicherheitsmaßnahmen zu begegnen, die sich aus dem „normalen“ Arbeitsalltag ergeben. Art. 32 Abs. 4 DS-GVO erwähnt daher explizit, dass die eigenen internen Abläufe im Betrieb so organisiert sein müssen, dass es auch dort nicht zu Sicherheitsverletzungen kommt. Hierzu ist insbesondere ein Berechtigungsmanagement sicherzustellen, damit ausscheidende Mitarbeiter nach Beendigung des Arbeitsverhältnisses oder sonstige unbefugte Dritte nicht auf Daten zugreifen können.

Eine geeignete Maßnahme zur Sicherheit der Verarbeitung ist gemäß Art. 32 Abs. 1a DS- GVO die Verschlüsselung der Kommunikation. So sollte zukünftig der E-Mail Verkehr oder etwa auch die Kommunikation über ein Kontaktformular auf der Homepage verschlüsselt werden.

Aufgrund der hohen Anforderungen empfiehlt sich, ein fachkundiges Unternehmen mit der Erstellung einer Analyse zu beauftragen.

VII. Pflicht zur Erstellung eines Verarbeitungsverzeichnisses

Unternehmen arbeiten in großen Mengen mit persönlichen Daten. Im Online-Handel geschieht dies vornehmlich mit sensiblen Anschriftsdaten oder Zahlungsinformationen (z. B. Kreditkartendaten). Zudem kommen die Daten der Angestellten hinzu. Grundsätzlich fordert Art. 30 DS-GVO, dass alle Verantwortlichen ein Verzeichnis über alle Verarbeitungstätigkeiten zu führen haben, die in ihrem Unternehmen durchgeführt werden. Es muss also dokumentiert werden, in welchem Zusammenhang mit personenbezogenen Daten gearbeitet wird. Von dieser Verpflichtung sind Unternehmen mit weniger als 250 Mitarbeitern befreit, sofern dort **nur gelegentlich** Daten verarbeitet werden. Dies ist aber schon dann nicht mehr der Fall, wenn etwa Mitarbeiterdaten für die Lohnbuchhaltung regelmäßig verarbeitet werden. In der Praxis ist somit **nahezu jedes Unternehmen** zur Erstellung eines so genannten Verfahrensverzeichnisses **verpflichtet**.

Das aufzustellende Verfahrensverzeichnis enthält u. a. die folgenden Angaben:

- den Namen und die Kontaktdaten des Verantwortlichen sowie des Datenschutzbeauftragten,
- die Zwecke der Datenverarbeitung,
- die Empfänger, gegenüber denen die Daten offengelegt worden sind oder noch offengelegt werden.

Ein Musterverzeichnis als Bearbeitungsgrundlage kann etwa über die Homepage des Landesbeauftragten für den Datenschutz Bayern abgerufen werden.

VIII. Der Datenschutzbeauftragte

Die DSGVO selbst trifft keine explizite Verpflichtung zur Benennung eines Datenschutzbeauftragten; dieser wird in der Verordnung vereinzelt erwähnt. Jedoch regelt das neue BDSG in § 38 BDSG eine Verpflichtung zur Benennung eines betrieblichen Datenschutzbeauftragten, wenn in der Regel **mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten** beauftragt sind. Dabei ist unerheblich, ob diese Personen Teilzeit- oder Vollzeitbeschäftigte sind, es zählen also die Personen. Auch freie Mitarbeiter oder Leiharbeitnehmer sind in die Berechnung einzubeziehen, ebenso Lehrlinge und Praktikanten.

Die gleiche Verpflichtung trifft diejenigen Unternehmen, deren Datenverarbeitung gemäß Art. 35 DSGVO einer Datenschutz-Folgenabschätzung bedarf. Dies sind Unternehmen, deren Datenverarbeitung mit hohen Risiken für die Rechte und Freiheiten der Betroffenen verbunden ist (sog. Risikodaten). Dies sind Unternehmen, die umfangreich besondere Kategorien personenbezogener Daten (vgl. Art 9 DSGVO), oder mit Daten arbeiten, anhand derer diese in persönlicher Hinsicht bewertet werden können (z. B. Kreditwürdigkeit). Schließlich müssen auch Unternehmen, welche eine umfangreiche Überwachung der öffentlich zugänglichen Bereiche vornehmen (**Videoüberwachung**), eine Datenschutz-Folgenabschätzung vornehmen und damit zugleich einen Datenschutzbeauftragten bestellen.

IX. Verträge über Auftragsverarbeitung, Art. 28 DSGVO

Häufig schalten unternehmen externe Dienstleister ein, die für das Unternehmen z. B. die IT-Einrichtung warten, die Buchhaltung erledigen oder auch die Kundenberatung übernehmen (Callcenter). Wenn Dienstleister derartige Aufgaben für andere erfüllen und bei der Erfüllung mit personenbezogenen Daten umgehen, spricht man von einer Auftragsverarbeitung, für welche ein gesonderter Vertrag zu schließen ist. Bei der Auftragsdatenverarbeitung erhebt, verarbeitet und/oder nutzt ein externer Dienstleister die personenbezogenen Daten für einen anderen, „Auftraggeber“, beispielsweise den Online-Händler. Vorteil einer

Auftragsdatenverarbeitung ist, dass der Auftraggeber (Unternehmer) weiterhin verantwortlicher für die Datenverarbeitung ist und bleibt, die Datenverarbeitung durch den Auftragnehmer somit keiner gesonderten Rechtfertigung, wie etwa einer Einwilligung durch den von der Datenverarbeitung Betroffenen bedarf.

Vor der Reformierung war die Auftragsdatenverarbeitung in § 11 BDSF a. F. geregelt. Nunmehr regelt Art. 28 DSGVO die **Mindestinhalte** einer Vereinbarung. Diese muss insbesondere das Weisungsrecht des Verantwortlichen festschreiben sowie die Aufgaben des Verantwortlichen beschreiben. Zudem muss der Auftragsverarbeiter zur Vertraulichkeit und Einhaltung der Sicherheit der Verarbeitung verpflichtet und festlegt werden, was mit den Daten nach Abschluss der Auftragsverarbeitung geschehen soll. Ergänzend regelt nunmehr § 62 BDSG die Auftragsdatenverarbeitung, wobei die Bedingungen an eine wirksame Auftragserteilung im Wesentlichen denjenigen aus Art. 28 DSGVO entsprechen.

Beispiele für eine Auftragsdatenverarbeitung sind:

- Werbeadressenverarbeitung in einem Lettershop
- dauerhafte oder temporäre Nutzung externer Serverkapazitäten
- Auslagerung des Kundenservices (z. B. Bestellannahme) an ein externes Callcenter
- Entsorgung von Datenträgern oder Akten
- Wartungsdienstleistungen von Servern und Computern bei Einsicht in personenbezogene Daten
- Nutzung von Google Analytics

Werden vorgenannte Dienste in Anspruch genommen, muss ab dem 25.05.2018 **zwingend eine Auftragsverarbeitungsvereinbarung abgeschlossen werden**.

Abzugrenzen ist die Auftragsverarbeitung von der Inanspruchnahme externer Fachleistungen. Bei diesen Leistungen muss kein Vertrag über eine Auftragsdatenverarbeitung abgeschlossen werden.

Die Abgrenzung ist im Einzelfall schwierig. Die Abgrenzung kann anhand folgender Kriterien vorgenommen werden:

- Ausführliche dem Auftragsverarbeiter wenig Spielraum gebende Weisungen (z. B. Speicherung der Daten auf Server)
- Sorgfältige und permanente Beaufsichtigung durch den Auftraggeber
- Auftreten des Auftragnehmers als verantwortliche Stelle (Beispiel: Call-Center, dass sich bei dem Kunden mit der Identität des Auftraggebers melden soll)
- Hohe Fachkompetenz des Dienstleisters (Beispiel: Anwälte, Steuerberater)
- Weiter Handlungsspielraum

Als Faustformel lässt sich sagen: Eine Auftragsverarbeitung i. S. v. Art. 24 DSGVO liegt dann vor, wenn allein das Unternehmen über Zwecke und Mittel der Verarbeitung entscheidet, d. h. der Auftragsverarbeiter weisungsabhängig den Auftrag erfüllt, er somit als „verlängerte Werkbank“ fungiert.

Als Beispiele für die Beauftragung externer Fachleistungen, für die in der Regel keine gesonderte Vereinbarung über eine Auftragsverarbeitung abzuschließen ist, können genannt werden:

- Externe Fachleistungen einer Personalverwaltung
- Mitarbeiterrekrutierung,
- Vertragskundenbetreuung
- Finanzberatung
- Rechtsanwälte
- Steuerberater (soweit nicht ausführlichen Weisungen unterworfen)
- Unternehmensberatung
- Wirtschaftsprüfung
- Inkassotätigkeit mit Forderungsübertragung.

X. Der neue Beschäftigtendatenschutz

Die DSGVO regelt den Datenschutz künftig europaweit einheitlich und ist vorrangig vor nationalem Recht anzuwenden. Allerdings darf der nationale Gesetzgeber aufgrund einer so genannten Öffnungsklausel (Art. 88 Abs. 2 DSGVO) eigene Regelungen zum Arbeitnehmerdatenschutz treffen, wovon der deutsche Gesetzgeber in der Neufassung von § 26 BDSG Gebrauch gemacht hat.

Die Neuregelung von § 26 BDSG ist umfangreicher als die bisherige Regelung zum Beschäftigtendatenschutz von § 32 BDSG, sie entspricht aber weitgehend der alten Rechtslage.

In der Vergangenheit wurde die Erlaubnis für die Datenverarbeitung vielfach durch eine Einwilligung des Arbeitnehmers herbeigeführt. Zwar ist auch weiterhin eine schriftliche Einwilligung des Arbeitnehmers zur Datenverarbeitung vorgesehen, zukünftig jedoch nur dann, wenn diese Einwilligung „freiwillig" abgegeben wird. Eine Freiwilligkeit der Einwilligung ist anzunehmen, wenn sie für die beschäftigte Person rechtlich oder wirtschaftlich vorteilhaft ist oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen, § 26 Abs. 2 BDSG. Bei im Raume stehenden Pflichtverstößen des Arbeitnehmers gegen seine arbeitsvertraglichen Verpflichtungen etwa sind Einwilligungen der Arbeitnehmer jedoch regelmäßig unfreiwillig. Arbeitgeber und Arbeitnehmer verfolgen keine gleichgelagerten Interessen, interne Ermittlungen sind für den Arbeitnehmer nachteilhaft, da sie dessen Kündigung beabsichtigen. Zudem hat der Arbeitgeber kein Interesse, Kontrollen zur Disposition des Beschäftigten zu stellen.

Damit wird insbesondere bei Kontrollmaßnahmen durch den Arbeitgeber der gesetzliche Erlaubnistatbestand von § 26 BDSG Bedeutung erlangt. Dieser erlaubt die Datenverarbeitung für **Zwecke der Beschäftigungsverhältnisse** und zur **Aufdeckung von Straftaten**.

a) Verarbeitung von Beschäftigtendaten zur Aufdeckung von Straftaten, § 26 Abs. 1 S. 2 BDSG

Die Verarbeitung von personenbezogenen Beschäftigtendaten zur Aufdeckung von Straftaten ist zulässig, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Arbeitnehmer eine Straftat begangen hat. Die beabsichtigte Datenverarbeitung, d. h. die beabsichtigte Kontrollmaßnahme muss zur Aufdeckung dieser Straftat erforderlich sein und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung darf nicht überwiegen. Dies entspricht im Wesentlichen der alten Rechtslage. Die Anforderungen an den Verdacht einer Straftat sind verhältnismäßig gering, ausreichend ist bereits ein einfacher Tatverdacht, der vor Beginn einer Untersuchung sorgfältig dokumentiert werden muss.

b) Verarbeitung von Daten für Zwecke des Beschäftigungsverhältnisses, § 26 Abs. 1 S. 1 BDSG

Die Datenverarbeitung und beabsichtigte Kontrollen bezwecken in der Praxis nicht immer die Aufklärung möglicher Straftaten. Auch die Aufklärung von Verstößen gegen arbeitsvertragliche Pflichten oder die Aufklärung tatsächlicher oder vermuteter Ordnungswidrigkeiten oder auch die beabsichtigte Begründung eines Arbeitsverhältnisses erfordern regelmäßig die Verarbeitung von Beschäftigtendaten. Diese Datenverarbeitungen können unter den Voraussetzungen des § 26 Abs. 1 S. 1 BDSG zulässig sein. Dies ist der Fall, wenn die Datenverarbeitung zur Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich sind. Dazu zählt auch die Aufklärung des Verdachts von Pflichtverletzungen des Arbeitnehmers, welche keine Straftaten sind. Neben anlassgebundenen Aufklärungsmaßnahmen können verdachtsunabhängige Kontrollen in den von der Rechtsprechung aufgestellten engen Grenzen nach § 26 Ans. 1 BDSG nF oder nach Art. 6 Abs. 1 f) DSGVO zulässig sein.

c) Erlaubnistatbestände der DSGVO

Neben dem Erlaubnistatbestand von § 26 Abs. 1 BDSG kann die Verarbeitung personenbezogener Daten auch nach der DSGVO gerechtfertigt sein, etwa nach Art. 6 Abs. 1 oder nach Art. 9 Abs. 2 DSGVO. Damit bleibt eine Datenverarbeitung zur Verwirklichung von Zwecken außerhalb des Beschäftigungsverhältnisses zulässig, etwa für Zwecke der Verfolgung, Durchsetzung und Abwehr von Ansprüchen. So kann etwa eine Revision des Unternehmens auf Art. 6 Abs. 1 c) oder f) DSGVO gestützt werden.

d) Betriebsvereinbarungen als Verarbeitungsgrundlage, § 26 Abs. 4 BDSG nF

Die Verarbeitung von Beschäftigungsdaten ist wie nach der bisherigen Rechtslage weiterhin auch auf der Grundlage von Kollektivvereinbarungen möglich. Sorgfältig formulierte Betriebsvereinbarungen als Basis für Kontrollen können datenschutzrechtliche Risiken erheblich reduzieren und eine Grundlage für rechtmäßige Kontrollen bilden.

XI. Fazit und Umsetzungsplanung

Unternehmen müssen wegen der so genannten Rechenschaftspflicht gemäß Art. 5 Abs. 2, 24 Abs. 1 DS-GVO den Nachweis erbringen können, die Anforderungen der Datenschutzverordnung umgesetzt zu haben. Dies erfordert viele organisatorische Maßnahmen und Prozesse, Mitarbeiter müssen im Datenschutz geschult und ein Datenschutzbeauftragter bestellt werden. Die Anforderungen der DS-GVO erfordern eine dauerhafte Umsetzung der datenschutzrechtlichen Vorschriften, so dass der Datenschutz keine einmalige Maßnahme, sondern kontinuierlicher Teil sämtlicher relevanter Prozesse eines Unternehmens ist. Das neue Recht stärkt die Rechte der Betroffenen und schafft hohe Risiken bei Verstößen. Die Umsetzung der hohen Anforderungen erfordert vielfach eine sorgfältige Analyse aller datenverarbeitenden Prozesse, so dass Unternehmen gut beraten sind, die fachkundige Beratung eines Datenschützers in Anspruch zu nehmen und sich im Zweifelsfall anwaltlich bei der Ausgestaltung neuer Datenschutzerklärungen und Auftragsverarbeitungsverträgen beraten zu lassen.

Diese Erörterung gehört zum WebBaecker Infodienst 26/2018 - www.webbaecker.de - erschienen am 29.06.2018
Autor: RA Tom-Christian Uhland, Gehrke Econ Rechtsanwaltsgesellschaft mbH - Isernhagen und Hannover - www.gehrke-econ.de