1. Wann ist das neue Recht anzuwenden?

Die Datenschutzgrundverordnung gilt ab dem 25. Mai 2018 (Art. 99 Abs. 2 DS-GVO).

Sie wirkt unmittelbar und direkt (Art. 288 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union).

- Bestehende Datenverarbeitungsverfahren müssen ab diesem Zeitpunkt dem neuen Recht entsprechen.
- Eine Auslegung des bis dahin geltenden Rechts „im Lichte der DS-GVO“ ist systematisch nicht möglich, da die Anwendung ausdrücklich erst zum genannten Zeitpunkt geregelt ist.
- Verantwortliche können sich aber schon jetzt auf das neue Recht vorbereiten: Umso besser, wenn Verfahren so angepasst werden, dass sie schon das neue Recht einhalten und ebenso das noch geltende Recht. Das ist oft möglich.

Die JI-Richtlinie tritt am 6. Mai 2018 in Kraft (Art. 64 JI-Richtlinie). Sie ist nicht unmittelbar anzuwenden, sondern in nationales Recht umzusetzen, das grundsätzlich auch ab dem 6. Mai 2018 anzuwenden ist (Art. 63 JI-Richtlinie).

2. Was ist der sachliche Anwendungsbereich?

Die Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 DS-GVO).

Die Verarbeitung ist in Art. 4 Nr. 2 DS-GVO definiert als jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Die Verordnung findet nach Art. 2 a) - d) DS-GVO keine Anwendung auf die personenbezogene Datenverarbeitung, welche

a) vom EU-Recht ausgenommen ist (mangels Gemeinschaftskompetenz, z.B. Geheimdienste)
b) unter die gemeinsame Außen- und Sicherheitspolitik oder
c) unter das „Haushaltsprivileg“ fällt (Datenverarbeitung durch natürliche Personen zur ausschließlich persönlichen oder familiären Tätigkeit) oder
d) in den Anwendungsbereich der JI-Richtlinie fällt (Datenverarbeitung durch zuständige Behörden zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten, zur Vollstreckung strafrechtlicher Sanktionen oder zum Schutz vor und zur Abwehr von Bedrohungen der öffentlichen Sicherheit).

Des Weiteren findet die Verordnung keine Anwendung auf die Verarbeitung personenbezogener Daten, welche unter die Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG) fällt. Die Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen (Art. 95 DS-GVO).

3. Was ist der räumliche Anwendungsbereich?

Der Anwendungsbereich des EU-Datenschutzrechts wird erheblich erweitert: Neben dem Niederlassungsprinzip gilt auch das neue Marktortprinzip.

Nach Art. 3 Abs. 1 DS-GVO findet die Verordnung Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union; dabei kommt es allein auf den Ort der Niederlassung an und nicht auf den Ort der Datenverarbeitung (Niederlassungsprinzip).

Art. 3 Abs. 2 DS-GVO normiert das Marktortprinzip: Danach gilt die Verordnung in den folgenden Fällen auch für Verantwortliche und Auftragsverarbeiter ohne Niederlassung in der EU:

a) Die Datenverarbeitung steht im Zusammenhang damit, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist.
b) b) Die Datenverarbeitung steht im Zusammenhang damit, das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

4. Was ist mit dem bisherigen Datenschutzrecht?

Die bisherige EU-Datenschutzrichtlinie 95/46(EG) wird mit dem Beginn des Anwendungszeitraums der DS-GVO, also mit Wirkung vom 25. Mai 2018, aufgehoben (Art. 94 DS-GVO).

Die DS-GVO gilt dann unmittelbar, soweit sie nicht Richtliniencharakter bzw. Öffnungsklauseln hat.

Es gilt ein Anwendungsvorrang des EU-Rechts vor nationalen Regelungen: Wenn eine nationale Rechtsvorschrift im Widerspruch zu einer EU-Rechtsvorschrift steht, ist die EU-Rechtsvorschrift anzuwenden. Das nationale Recht bleibt formell gültig, es wird insoweit aber seine verbindliche Wirkung ausgesetzt (vgl. u. a. die **Costa/Enel - Entscheidung des EuGH vom 15.7.1964 – AZ. 6/64**).

Bundes- und Landesgesetzgeber sind deshalb aufgefordert, das bestehende Recht zu überarbeiten, um die rechtsichere Anwendung zu erleichtern.

5. Was hilft bei der Auslegung?

Die Erwägungsgründe der Verordnung können zur Auslegung herangezogen werden. Sie entfalten zwar keine unmittelbare normative Wirkung, verdeutlichen aber Motive und bieten Erläuterungen.

Auch die Vorentwürfe der EU-Gremien sind eine Quelle für Auslegungsmaterial; diese können herangezogen werden, vor allem um zu erkennen, was man gerade oder gerade eben nicht regeln wollte.

6. Gibt es noch nationale Regelungsspielräume?

Ja: Neben den an verschiedenen Stellen in der DS-GVO normierten Regelungsaufträgen, welche zwingend auf nationaler Ebene umzusetzen sind, gibt es in der DS-GVO viele Öffnungsklauseln, aufgrund derer die Mitgliedstaaten ergänzende Vorschriften einführen oder aufrechterhalten können.

Die Gesetzgebungsverfahren in Bund und Ländern sind noch im Gange. Es bleibt abzuwarten, inwieweit und in welcher Form von den Regelungsmöglichkeiten Gebrauch gemacht wird.

7. Welche Datenschutzbehörde ist zuständig?

Nach Art. 55 Abs.1 DS-GVO ist jede Aufsichtsbehörde für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig.

Unternehmen und andere nicht-öffentliche Stellen

Für Unternehmen und andere nicht-öffentliche Stellen in Deutschland sind grundsätzlich weiterhin die örtlich zuständigen Landesaufsichtsbehörden zuständig, es sei denn, es liegt eine Sonderzuständigkeit der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vor. Dies ist im Bereich Telekommunikations- und Postdienstleistungen der Fall.

Wenn es um eine grenzüberschreitende Verarbeitung geht, gilt das neue sogenannte „One-Stop-Shop"-Verfahren: Die Behörde am Sitz der Hauptniederlassung hat eine federführende Zuständigkeit. Unternehmen müssen sich also nicht mehr mit Aufsichtsbehörden in mehreren EU-Mitgliedstaaten als Ansprechpartner auseinandersetzen (Art. 56 DS-GVO).

Sogenannte „lokale Fälle" sind davon ausgenommen: Hängt der Gegenstand der Beschwerde ausschließlich mit der Niederlassung eines Mitgliedstaats zusammen oder wirkt sich die Datenverarbeitung nur auf betroffene Personen in diesem Mitgliedstaat aus, so ist jede Aufsichtsbehörde „lokal" zuständig (Art. 56 Abs. 2 DS-GVO).

Unabhängig davon können sich betroffene Personen mit Beschwerden an jede Behörde wenden.

Beim „Marktortprinzip" (Sitz im Drittstaat, keine Niederlassung in der EU) muss es - mangels Hauptniederlassung - dabei bleiben, dass jede Behörde zuständig ist.

Die Begriffe „grenzüberschreitende Verarbeitung", „Hauptniederlassung" und „betroffene Behörde" sind in Art. 4 Nr. 16, 22, 23 DS-GVO definiert.

Behörden

Für den öffentlichen Bereich ist der Sitz der Behörde entscheidend (Art. 55 Abs. 2 DS-GVO). In Deutschland verbleibt es insoweit bei der geltenden Zuständigkeitsverteilung zwischen Bund und Land.
Die Aufsichtsbehörden sind nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

8. Wie arbeiten die deutschen und die europäischen Aufsichtsbehörden zusammen?

Die europäischen Aufsichtsbehörden stimmen sich untereinander verbindlich ab. Dafür gibt es neu geregelte Verfahren, die ab Mai 2018 anzuwenden sind.

Zusammenarbeit bei grenzüberschreitenden Einzelfällen: („One-Stop-Shop“, Art. 60 DS-GVO)

Bei Fällen mit grenzüberschreitender Wirkung stimmen sich die beteiligten Behörden nach dem in Art. 60 DS-GVO formell geregelten Verfahren untereinander ab, um eine einheitliche Lösung zu finden.

Ausnahmsweise ist jede Aufsichtsbehörde dafür zuständig, sich mit einer bei ihr eingereichten Beschwerde oder einem etwaigen Verstoß gegen die DS-GVO zu befassen, wenn der Gegenstand nur mit einer Niederlassung in ihrem Mitgliedstaat zusammenhängt oder betroffene Personen nur ihres Mitgliedstaats erheblich beeinträchtigt. Auch in einem solchen Fall mit lediglich lokaler Auswirkung stimmen sich die Aufsichtsbehörden untereinander ab, um eine einheitliche Vorgehensweise zu erarbeiten (Art. 56 DS-GVO).

Daneben kann eine Aufsichtsbehörde eine andere Aufsichtsbehörde um Amtshilfe ersuchen oder es können mehrere Aufsichtsbehörden gemeinsame Maßnahmen durchführen (Art. 61, 62 DS-GVO).

Kohärenzverfahren (Art. 63 ff. DS-GVO):

Das Kohärenzverfahren im Europäischen Datenschutzausschuss folgt auf die Zusammenarbeit im Einzelfall, wenn keine Einigkeit zwischen den Aufsichtsbehörden erzielt werden konnte (Art. 60 Abs. 4 DS-GVO) und in grundsätzlichen Fragestellungen.

Der Ausschuss besteht aus den Leitern der Aufsichtsbehörden jedes Mitgliedstaates und dem Europäischen Datenschutzbeauftragten (Art. 68 Abs. 3 DS-GVO).

Wie die Zusammenarbeit der deutschen Aufsichtsbehörden und ihre Rolle in den neuen Verfahren sowie die Vertretung der Aufsichtsbehörden des Bundes und der Länder im Datenschutzausschuss im Einzelnen ausgestaltet wird, ist derzeit noch offen.

9. Was sind personenbezogene Daten?

“Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen (Art. 4 Nr. 1 DS-GVO).

Neu ist, dass bestimmte Merkmale wie Standortdaten, Online-Kennung sowie genetische Identität erwähnt werden. Dazu ist auf Erwägungsgrund 30 der DS-GVO hinzuweisen:

„Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die ihr Gerät oder Software-Anwendungen

und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren."

Ob und inwieweit die neue EuGH-Rechtsprechung zu IP-Adressen Auswirkungen hat und was dies für die Praxis und das neue Recht genau bedeutet, ist noch zu klären (vgl. **Urteil des EuGH vom 19.10.2016, Az. C-582/14 „Breyer vs. Bundesrepublik Deutschland**").

10. Wann ist eine personenbezogene Datenverarbeitung zulässig?

Es bleibt auch nach den neuen Regelungen der DS-GVO bei dem datenschutzrechtlichen Verbot mit Erlaubnisvorbehalt. Danach ist eine personenbezogene Datenverarbeitung verboten, soweit keine gesetzliche Erlaubnisregelung diese gestattet oder eine Einwilligung der betroffenen Person vorliegt, welche die Verarbeitung ihrer Daten legitimiert (Art. 6 Abs. 1 DS-GVO).

Einwilligung

Damit bleibt die Einwilligung ein zentrales Legitimationsmittel für die Datenverarbeitung.

Sie ist definiert als „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" (Art. 4 Nr. 11 DS-GVO). Bedingungen, die eine Einwilligung erfüllen muss, sind in den Arti. 7 und 8 DS-GVO definiert.

Bereits nach bisherigem Recht erteilte Einwilligungen können weiter gelten, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 DS-GVO).
Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen. Informationspflichten nach Art. 13 DS-GVO müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.

Besondere Beachtung verdienen allerdings die folgenden Bedingungen der DS-GVO; sind diese Bedingungen nicht erfüllt, gelten bisher erteilte Einwilligungen nicht fort:

- Freiwilligkeit („Kopplungsverbot", Art. 7 Abs. 4 in Verbindung mit Erwägungsgrund 43 DS-GVO),

- Altersgrenze: 16 Jahre (soweit im nationalen Recht nichts anderes bestimmt wird; Schutz des Kindeswohls, Art. 8 Abs. 1 in Verbindung mit Erwägungsgrund 38 DS-GVO).

Verantwortliche Stellen müssen in der Übergangsphase bis Mai 2018 prüfen, ob deren eingeholte Einwilligungen der Art nach den Bedingungen der DS-GVO entsprechen. Dies beinhaltet datenschutzrechtliche Grundsätze wie Transparenz und Zweck der Verarbeitung der personenbezogenen Daten. Mindestanforderung ist, dass eine bislang eingeholte Einwilligung momentan rechtswirksam ist.

Unabhängig davon gilt selbstverständlich, dass ab dem 25. Mai 2018 sämtliche Voraussetzungen nach der DS-GVO – und damit auch u. a. die Informationspflichten und Datenschutzgrundsätze, wie „Privacy by Design“ – durch die Unternehmen umgesetzt werden müssen. Vor diesem Hintergrund empfehlen die Aufsichtsbehörden den Unternehmen, bei den bestehenden Einwilligungen in der Übergangsphase bis Mai 2018 die Vorgaben zu den Informationspflichten gemäß Art. 7 Abs. 3 S. 3, 13 und 14 DS-GVO nachzuholen.

Die Gesamtthematik der Einwilligung wird in den Arbeitsgremien der Datenschutzkonferenz weiter bearbeitet. Es ist zu erwarten, dass aus den Arbeitsergebnissen weitere Konkretisierungen entstehen, die zügig veröffentlicht werden.

Vgl. hierzu den **Beschluss des Düsseldorfer Kreises vom 13./14.09.2016**.

Rechtsgrundlagen

Die allgemeinen Rechtsgrundlagen für personenbezogene Datenverarbeitungen finden sich in Art. 6 Abs. 1 DS-GVO.

Für den nicht öffentlichen Bereich ist meist Art. 6 Abs.1 Buchstabe f) DS-GVO maßgeblich. Danach ist eine Verarbeitung zulässig, wenn sie zur Wahrung der berechtigten 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, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Für den öffentlichen Bereich gilt, dass die Rechtsgrundlagen durch das nationale Recht festgelegt werden (Art. 6 Abs. 3 DS-GVO). Insoweit hat Art. 6 Abs. 3 DS-GVO Richtliniencharakter: Der nationale Gesetzgeber ist hier gefragt, die einzelnen Vorgaben (Zweck, welche Art von Daten, welche allgemeinen Bedingungen usw.) verbindlich zu regeln.

Die Rechtsgrundlage bei Verarbeitung besonderer Kategorien von personenbezogenen Daten bildet Art. 9 DS-GVO. Die Mitgliedstaaten können zusätzli-

che Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist (Art. 9 Abs. 4 DS-GVO).

Aufgrund zahlreicher Öffnungsklauseln im Verordnungstext wird es den Mitgliedstaaten in vielen Bereichen selbst überlassen, weitergehende nationale Regelungen zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Daten zu treffen:

- Art. 85 DS-GVO Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit,
- Art. 86 DS-GVO Verarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten,
- Art. 88 DS-GVO Datenverarbeitung im Beschäftigungskontext,
- Art. 89 DS-GVO Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen,
  oder historischen Forschungszwecken und zu statistischen Zwecken
- Art. 90 DS-GVO Geheimhaltungspflichten,
- Art. 91 DS-GVO Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften.

Die Gesetzgebungsverfahren in Bund und Ländern sind noch im Gange. Es bleibt abzuwarten, inwieweit und in welcher Form von den Regelungsverpflichtungen und -möglichkeiten Gebrauch gemacht wird.

11. Welche Sanktionen und Durchsetzungsmöglichkeiten gibt es nach der DS-GVO?

Die DS-GVO will effektiv und zielgerichtet mittels empfindlicher Sanktionen den einheitlichen Standard in Europa für alle dort wirtschaftlich Tätigen verwirklichen. Der Bußgeldrahmen wird deutlich erhöht. Behördliche Maßnahmen können zukünftig nicht nur gegen den für die Verarbeitung Verantwortlichen selbst, sondern auch gegen Auftragsverarbeiter gerichtet werden. Die Aufsichtsbehörden können – anders als bisher – auch gegenüber Behörden Maßnahmen verbindlich anordnen.

Sanktionen und Durchsetzungsmöglichkeiten der Aufsichtsbehörden

Um Verstöße zu ahnden, steht den Aufsichtsbehörden unter der DS-GVO ein breites Spektrum an Maßnahmen zur Verfügung. Zunächst können vorsorgliche Warnungen (Art. 58 Abs. 2 Buchstabe a DS-GVO) an verantwortliche Stellen und Auftragsverarbeiter ausgesprochen werden, wenn diese Datenverarbeitungen beabsichtigen, die voraussichtlich einen Verstoß gegen die Grund-

verordnung darstellen bzw. Verwarnungen (Art. 58 Abs. 2 Buchstabe b DS-GVO), wenn mit solchen Datenverarbeitungen bereits gegen die DS-GVO verstoßen wurde.

Darüber hinaus können Verantwortliche künftig von den Aufsichtsbehörden formal angewiesen werden, Betroffenenrechten zu entsprechen (Art. 58 Abs. 2 Buchstabe c DS-GVO), Datenverarbeitungen mit der Grundverordnung in Einklang zu bringen (Art. 58 Abs. 2 Buchstabe d DS-GVO) sowie von einem Datenschutzverstoß betroffene Personen zu benachrichtigen (Art. 58 Abs. 2 Buchstabe e DS-GVO).

Ausdrücklich kann künftig auch die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland angeordnet werden (Art. 58 Abs. 2 Buchstabe j DS-GVO). Wie bisher können Aufsichtsbehörden weiterhin Beschränkungen und Verbote von Datenverarbeitungen verhängen (Art. 58 Abs. 2 Buchstabe f DS-GVO) sowie die Berichtigung und Löschung bestimmter Daten, sowie eine Einschränkung der Verarbeitung solcher Daten anordnen (Art. 58 Abs. 2 Buchstabe g DS-GVO). Zertifizierungsstellen können angewiesen werden, erteilte Zertifizierungen zu widerrufen oder neue Zertifizierungen nicht zu erteilen (Art. 58 Abs. 2 Buchst. h).

Zusätzlich oder anstelle dieser Maßnahmen können Verstöße gegen die DS-GVO auch weiterhin mit Geldbußen geahndet werden.

Die Aufsichtsbehörden haben die Befugnis, alle Informationen zu verlangen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Hierzu können sie den für die Verarbeitung Verantwortlichen, den Auftragsverarbeiter und den Vertreter des für die Verarbeitung Verantwortlichen anweisen.

Bußgeldrahmen und Bußgeldzumessung

Bußgelder müssen wirksam, verhältnismäßig und abschreckend sein. Der Bußgeldrahmen wird mit der DS-GVO deutlich erhöht. So können Bußgelder bei schweren Verstößen Höhen von bis zu 20.000.000 Euro erreichen. Gegen Unternehmen kann diese Grenze sogar noch überschritten werden, nämlich bis zu 4 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres (Art. 83 DS-GVO).

Für die konkrete Bestimmung der Höhe eines Bußgeldes wird eine Vielzahl von Aspekten einzubeziehen sein. Dabei ist neben Art, Schwere und Dauer des Verstoßes unter anderem auch zu berücksichtigen, welche Art von Daten verarbeitet wurde, ob früher angeordnete Maßnahmen von der verantwortlichen Stelle eingehalten wurden sowie ob und welche Vorteile durch die Datenverarbeitung erlangt wurden. Es wird auch zu berücksichtigen sein, ob und wie die verantwortlichen Stellen mit den Aufsichtsbehörden zusammengearbeitet haben, um Verstößen abzuhelfen und ob sie die Verstöße eigenständig mitgeteilt haben.