NOERR

Data Compliance Compass

Navigieren Sie sicher durch die Datenlandschaft

Juni 2024

Data Compliance Compass

In der heutigen datengetriebenen Welt ist die Einhaltung von europäischen und nationalen Vorschriften für den Datenverkehr für Unternehmen aller Größenordnungen von entscheidender Bedeutung. Die Nichteinhaltung kann zu erheblichen Bußgeldern, Reputationsverlusten und sogar zu rechtlichen Schritten führen.

Der Data Compliance Compass soll Ihnen einen Überblick über besonders relevante Rechtsakte verschaffen und Ihnen die wichtigsten Pflichten, die sich daraus ergeben, aufzeigen.

Inhalt

Data Compliance Compass 1

Europäische Rechtsakte 3

Einführung 3
Überblick der wichtigsten europäischen Rechtsakte 4
Die europäischen Regelungen im Einzelnen 5
Digital Markets Act (DMA) 6
Data Act 8
DS-GVO 10
Data Governance Act (DGA) 12
Digital Service Act (DSA) 14
AI Act 16
Open Data Directive 18
e-Privacy-Verordnung 19
Free-Flow-of-Data-Verordnung 20

Nationale Rechtsvorschriften 21

Einfühlung 21
Überblick über die wichtigsten nationalen Rechtsakte 21
Die nationalen Rechtsakte im Einzelnen 21
GeschGehG 22
BDSG 24
DDG 26
TTDDDG 28
UrhG 29
UrhDaG 30
TKG 31
StGB 33

Europäische Rechtsakte

Einführung

Der europäische Gesetzgeber hat in den letzten Jahren als Reaktion auf den enormen gesellschaftlichen Wandel, den der digitale Fortschritt verursacht hat, die Regulierung der Daten- und Digitalwirtschaft aktiv vorangetrieben. Am 19.02.2020 veröffentlichte die Europäische Kommission in diesem Zusammenhang eine Europäische Datenstrategie, welche die EU an die Spitze einer datengesteuerten Gesellschaft bringen soll.

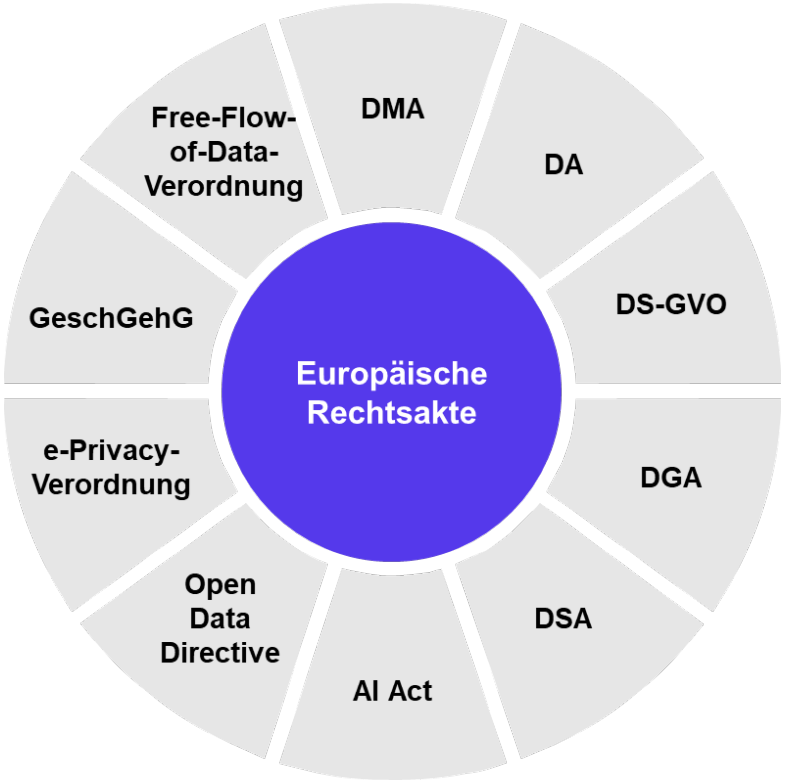
Dabei sollen die durch die Datenwirtschaft geschaffenen Chancen möglichst effektiv genutzt werden, indem nationale Barrieren abgebaut und Verfügbarkeit, Transparenz und Interoperabilität von Daten gefördert werden. Diese Vorhaben werden, unter anderem durch den Erlass des Data Act („DA“), des Data Governance Act („DGA“) und der Open Data Directive vorangetrieben.

Gleichzeitig ließ der EU-Gesetzgeber das gesellschaftliche Risiko in Bezug auf die (systemische) Gefährdung von Grundfreiheiten v. a. im Bereich personenbezogener Daten in die Abwägung einfließen und erließ als Reaktion darauf die Datenschutzgrundverordnung („DS-GVO“), den Digital Services Act („DSA") und den AI Act.

Auch der Macht der Big Player auf dem Markt (Gatekeeper) soll durch den Digital Markets Act („DMA“) sowie die Anwendung kartellrechtlicher Vorschriften die Stirn geboten werden.

Wenngleich die neuen Gesetzesakte – in jüngster Zeit vor allem der DSA – viele Herausforderungen in Bezug auf Data Compliance bergen, so möchten wir Ihnen mit dem DATA COMPLIANCE COMPASS Data Compliance Compass auch die Chancen und wesentlichen Pflichten aufzeigen, die eine Schaffung eines Rechtsrahmens für die Daten- und Digitalwirtschaft mit sich bringt.

Überblick der wichtigsten europäischen Rechtsakte



- **DMA:** Kartellrechtsnahe Vorschriften zur Begrenzung der Marktmacht der sog. Gatekeeper in der Digitalwirtschaft
- **DA**: Förderung der Wertschöpfung von Daten durch Datenzugangsrechte, inklusive Vertragsrecht für Daten, aber auch öffentlich-rechtliche Vorschriften zum Datenzugang
- **DS-GVO:** Schutz von personenbezogenen Daten
- **DGA:** Förderung der Verfügbarkeit von Daten, vor allem durch Förderung der Weitergabe von geschützten öffentlichen Daten z. B. für die Forschung
- **DSA:** Schutz von Grundrechten (und Grundfreiheiten) im Internet durch die Bekämpfung rechtswidriger Inhalte
- **AI Act:** Schutz vor Risiken, die KI für die Grundrechte natürlicher Personen birgt
- **Open Data Directive:** Bereits öffentliche Daten im Besitz von öffentlich-rechtlichen Körperschaften sollen möglichst einfach und barrierefrei verfügbar sein
- **e-Privacy-Verordnung:** Soll aufbauend auf der DS-GVO den Schutz personenbezogener Daten im elektronischen Kommunikationsbereich verbessern
- **GeschGehG:** Schutz von Geschäftsgeheimnissen durch zivilrechtliche Ansprüche und strafrechtliche Sanktionen gegen Schädigenden
- **Free-Flow-of-Data-Verordnung**: Beseitigung von Datenverkehrshindernissen, vor allem durch das Verbot von nationalen Datenlokalisierungsauflagen

Die europäischen Regelungen im Einzelnen

Legende:

	Rechtsakt bezieht sich auf nicht-personenbezogene Daten
	Rechtsakt bezieht sich auf personenbezogene Daten
	Rechtsakt ist in Kraft
	Rechtsakt ist beschlossen, aber noch nicht in Kraft
	Rechtsakt befindet sich im Gesetzgebungsverfahren

Digital Markets Act (DMA)

Kurzumriss:

Mit dem Digital Markets Act („DMA“) wird das Verhalten bestimmter großer Digitalkonzerne (sog. „Gatekeeper“) reguliert, die Plattformdienste in der Digitalwirtschaft anbieten und welche aufgrund ihrer Position als wichtige Zugangstore von gewerblichen Nutzern zu Endnutzern dienen. Die Unternehmen müssen zudem, um als Gatekeeper eingestuft zu werden, erheblichen Einfluss auf den Binnenmarkt haben, sowie in ihren Tätigkeiten eine gefestigte und dauerhafte Stellung haben oder absehbar erlangen. Es gilt eine Vermutungsregelung bei Überschreiten von quantitativen Schwellenwerten (bzgl. Jahresumsatz/Marktkapitalisierung sowie Nutzerzahlen).

Durch den DMA soll die Bestreitbarkeit und Fairness von Märkten im Digitalsektor soll sichergestellt werden, indem Gatekeepern umfangreiche (u. a. datenbezogene) Verhaltenspflichten auferlegt werden.

Primärer (datenrechtlicher) Adressat der Regulierung:

Adressat des DMA sind die Betreiber sog. „zentraler Plattformdienste“, die gewerblichen Nutzern als Zugangstor zu Endnutzern dienen. Zu zentralen Plattformdiensten zählen beispielsweise Online-Vermittlungsdienste, Online-Suchmaschinen, soziale Netzwerke, Betriebssysteme, Webbrowser, etc. Der DMA findet auf diese Anwendung, **wenn und soweit** die Betreiber durch die Europäische Kommission als Gatekeeper eingestuft wurden.

Es sind alle Dienste erfasst, die in der EU angeboten werden. Der Firmensitz ist unerheblich.

Datenbezogene Verhaltenspflichten beinhalten u.a. Nutzungsverbote für Daten, Verpflichtungen zur Herstellung von Interoperabilität und Datenzugangsansprüche gewerblicher Nutzer, Endnutzer und Dritter ggü. den Gatekeepern.

Pflichten/Anforderungen/Risiken in Bezug auf Daten:

Was ist das Verhältnis zu anderen Vorschriften?

– Der DMA gilt grundsätzlich parallel zu bestehenden kartellrechtlichen Vorschriften auf nationaler und EU-Ebene (Art. 1 Abs. 6 DMA), gleichzeitig wird eine Fragmentierung von Regelungen ggü. Gatekeepern untersagt (Art. 1 Abs. 5 DMA).

Welche Pflichten werden hinsichtlich der Daten aufgestellt?

– Umfassender, unmittelbar geltender Pflichtenkatalog in Art. 5 - 6 DMA, abgeleitet aus kartellrechtlicher Entscheidungspraxis der letzten 20 Jahre, u. a.: Selbstbegünstigungsverbote, Regelungen zur Datennutzung und zur Dateninteroperabilität, Diskriminierungsverbote, Informationsherausgabepflichten, Datenkombinationsverbote, (Daten-)Zugangsansprüche).

– Art. 7 DMA normiert eine Interoperabilitätspflicht für nummernunabhängige interpersoneller Kommunikationsdienste (z. B. Whatsapp).

– Art. 14 Abs. 1 DMA verpflichtet die Gatekeeper unter bestimmten Voraussetzungen zur Unterrichtung der EU-Kommission über Zusammenschlussvorhaben i. S. d. Art. 3 FKVO. Es besteht jedoch keine Genehmigungspflicht.

– Die Art. 20 ff. DMA verleihen der EU-Kommission kartellrechtsübliche Untersuchungsbefugnisse: Einleitung von Verfahren, Auskunftspflichten, Nachprüfungen bei Unternehmen und Verhängung von Abhilfemaßnahmen.

– Auch Dritte sind dazu berufen, die Compliance der Gatekeeper mit dem DMA zu überwachen, , etwa durch Beschwerden bei der EU-Kommission (auch über Whistleblower Tool), aber auch durch Private Enforcement vor nationalen Gerichten.

Welche Sanktionen sind für Pflichtverletzungen vorgesehen (Risiko)?

– Bei Verstößen: Bußgelder von bis zu 10 %, bei Wiederholung bis zu 20 % des weltweiten Jahresumsatzes (Art. 30 ff. DMA) sowie bei systematischer Nichteinhaltung sogar strukturelle Abhilfemaßnahmen.

Praktische Hinweise:

Der Anwendungsbereich des DMA ist – insbesondere aufgrund der hohen quantitativen Schwellen für die Vermutung der Stellung als Gatekeeper (Art. 3 Abs. 2 DMA) – relativ klein. Bisher wurden lediglich sieben Gatekeeper benannt (Alphabet, Amazon, Apple, Booking, ByteDance, Meta und Microsoft). Sofern die Schwellenwerte überschritten und ein Unternehmen von der EU-Kommission als Gatekeeper benannt wurde, muss die Compliance mit den Verhaltenspflichten des DMA (inkl. datenbezogener Pflichten) innerhalb von sechs Monaten nach der Benennung hergestellt (Art. 3 Abs. 10 DMA) und u. a. in einem Compliance-Report nachgewiesen werden (Art. 8 Abs. 1 DMA).

Unternehmen, die nicht selbst als Gatekeeper in Frage kommen, ist die Prüfung eigener Handlungsoptionen nach dem DMA zu empfehlen. Das betrifft insbesondere Datenzugangsansprüche und von den Gatekeepern bereits eingeräumte Datenzugänge, die für das eigene Geschäftsmodell nützlich sein können. Auch sollte die Compliance der Gatekeeper mit dem DMA laufend überwacht werden, um gegen Verhalten vorgehen zu können, das für das eigene Unternehmen schädlich ist.

Data Act

Kurzumriss:

Die EU zielt mit dem Data Act auf eine gerechte Verteilung der mit Daten verbundenen und bislang weitestgehend ungenutzten Wertschöpfung von Daten ab.

Der Data Act soll die für die bislang unzureichende Nutzung von Daten verantwortlichen rechtlichen, wirtschaftlichen und technischen Hindernisse beseitigen und somit eine stärkere Datennutzung und eine florierende Datenwirtschaft in der EU fördern, indem die rechtlichen Rahmenbedingungen des Datenzugangs und deren Förderung neu geregelt werden.

Während bisherige rechtliche Regelungen zu Daten vor allem auf ihren Schutz ausgerichtet waren, stößt der Data-Act vor diesem Hintergrund gerade in die entgegengesetzte Richtung vor und zielt auf die kommerzielle Nutzbarkeit der Daten ab.

Unter anderem sollen Zugangsrechte zu Daten für die Privatwirtschaft und den öffentlichen Sektor begründet werden.

Inkrafttreten: 11.01.2024

Primärer (datenrechtlicher) Adressat der Regulierung:

Art. 1 Abs. 3 DA legt die Adressaten des DA fest: potenziell betroffen ist nahezu jedes in der EU aktive Unternehmen, das Daten sammelt, verarbeitet, in ihren Produkten nutzt oder die damit im Zusammenhang stehenden Dienstleistungen anbietet.

Beispielsweise: Anbieter von IoT-Produkten (Art. 3 - 5 DA), auch Produkthersteller, Cloud-Anbieter, insgesamt alle Arten von Dateninhabern.

Es sind alle in der EU aktiven Dienste unabhängig vom Firmensitz erfasst und die Geltung grundsätzlich sektor- und branchenübergreifend.

Klein- und Kleinstunternehmen werden privilegiert, indem sie von den Pflichten des Kapitels II (Datenweitergabepflichten) ausgenommen werden.

Pflichten/Anforderungen/Risiken in Bezug auf Daten:

Was ist datenrechtlich geregelt?

– Der Data Act umfasst fünf wesentliche Regelungsgegenstände für den Zugang zu und die Verwendung von Daten in der EU:

1. Anspruch der Nutzer von IoT-Geräten und damit verbundenen Diensten auf Zugang und Nutzung nutzergenerierter Daten (sowohl Datenaustausch B2B als auch B2C) (Art. 3 - 5 DA)

2. Verbot unfairer Vertragsklauseln in standardisierten Datenlizenzverträgen zur Verhinderung des Missbrauchs vertraglicher Ungleichgewichte in Verträgen mit Unternehmen (Art. 13 DA) – eine Art B2B-AGB-Kontrolle

3. Recht auf Datenzugang und Datennutzung durch öffentliche Stellen (B2G) (Art. 14 - 22 DA)

4. Erleichterung des Wechsels von einem Datenverarbeitungsdienst zum anderen (insb. Cloud- und Edge-Anbieter), Einführung von Schutzmaßnahmen gegen unrechtmäßige Datenübertragungen (Art. 23 - 26 DA)

5. Anforderungen an die Interoperabilität von Datenverarbeitungsdiensten, sowie an die internationale Datenübertragung, Schutz vor Zugriff von Drittstaaten (Art. 27 - 32 DA)

Welche weiteren Ansprüche und Pflichten werden hinsichtlich der Daten aufgestellt?

– IoT-Geräte müssen so konzipiert und hergestellt, und verbundene Dienste so konzipiert und erbracht werden, dass Produkt- und Dienstdaten standardmäßig für den Nutzer einfach, sicher, unentgeltlich, in einem umfassenden maschinenlesbaren Format verfügbar sind (Art. 3 Abs. 1 DA) = „accessibility by design“

– vorvertragliche Informationspflichten bezüglich des Umfangs und der Speicherung sowie der Zugriffsmöglichkeiten auf die generierten Daten eines IoT-Gerätes und damit verbundenen Dienstes (Art. 3 Abs. 2 - 3 DA)

– Nutzer müssen unentgeltlich auf Daten zugreifen können (Art. 4 Abs. DA)

– Soweit der Nutzer Datenbereitstellung an Dritte verlangt, darf der Dritte diese allerdings nur zur Erfüllung seiner Pflichten gegenüber dem Nutzer verwenden und muss sie danach löschen (Art. 6 DA)

– Gegenleistungen, die der Dateninhaber für die Bereitstellung seiner Daten gegenüber Datenempfängern erhält, müssen der Höhe nach bei Datenlizenzverträgen zwischen Unternehmern angemessen und diskriminierungsfrei ausgestaltet sein (Art. 9 Abs. 1 DA)

– Ein Anbieter einer Anwendung, in der intelligente Verträge (smart contracts) verwendet werden, muss die wesentlichen Anforderungen des Art. 36 DA erfüllen

Welche Sanktionen sind für Pflichtverletzungen vorgesehen (Risiko)?

– Festlegung durch die Mitgliedstaaten. Möglich sind Geldbußen von bis zu EUR 20.000.000 bzw. bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes

Praktische Hinweise:

Im Rahmen des Projekts der Implementierung des Data Acts sollte zunächst eruiert werden, ob durch das Unternehmen IoT-Produkte (und damit verbundene Dienste) vertrieben werden, die in den Anwendungsbereich des Data Act fallen – für die Definition siehe Art. 2 Nr. 5 DA. Im Anschluss gilt es sodann, zu evaluieren, wo dringendster Handlungsbedarf besteht und wie die Pflichten des Data Acts auf Grundlage eines holistischen Ansatzes umgesetzt werden können. Dabei sollte der Fokus zunächst auf denjenigen Pflichten liegen, die Auswirkungen auf die Entwicklung sowie das Produktdesign haben (z.B. Access by Design).

Die zu entwickelnde Data Act-Strategie hat dabei auch Prozesse im Hinblick auf Datenherausgabeverlangen zu erfassen. Wichtig ist zu wissen, dass Geschäftsgeheimnisse unter bestimmten, allerdings hohen Voraussetzungen nicht offenbart werden müssen (Art. 4 Abs. 6 - 9 DA). Ebenso ist laut Erwägungsgrund 116 DA auf die kartellrechtlichen Grenzen des Datenaustauschs zu achten (kartellrechtliches Verbot des Informationsaustauschs, § 1 GWB bzw. Art. 101 AEUV).

Zudem ist zu empfehlen, technische Schutzmaßnahmen für die unbefugte Datennutzung bei Bereitstellung an Dritte (Art. 5 DA) zu ergreifen, was im Rahmen von Datenlizenzverträgen grundsätzlich erlaubt ist (Art. 11 DA).

DS-GVO

Kurzumriss:

Die DS-GVO regelt einheitlich die rechtlichen Vorgaben zur Verarbeitung personenbezogener Daten in der EU. Mit der Verordnung verfolgt die Union das Ziel, den Datenschutz in der EU einheitlich zu regeln, um einen Flickenteppich abweichender Regelungen in den verschiedenen EU-Ländern zu vermeiden. Stattdessen gilt seit 2018 in der gesamten EU ein einheitliches Datenschutzniveau. Von der Vollharmonisierung ausgenommen sind lediglich Bereiche, in denen die verschiedenen EU-Länder aufgrund sog. Öffnungsklauseln in der DS-GVO abweichende Regelungen erlassen können. Dies ist etwa im Arbeitsrecht und für die Verarbeitung von Gesundheitsdaten der Fall.

Erklärtes Ziel ist der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, und zugleich die Gewährleistung des freien Verkehrs solcher Daten (Art. 1 Abs. 1 DS-GVO).

Geschützt werden sollen dadurch die Grundrechte natürlicher Personen.

Primärer (datenrechtlicher) Adressat der Regulierung:

Primärer Adressat der DS-GVO sind die „Verantwortlichen“, d. h. natürliche oder juristische Personen, Behörden oder andere Stellen, die allein oder gemeinsam mit anderen über die Verarbeitung von personenbezogenen Daten entscheiden (Art. 4 Nr. 7 DS-GVO). Daneben werden auch die Tätigkeiten von Auftragsverarbeitern erfasst, die Daten im Auftrag des Verantwortlichen verarbeiten (Art. 4 Nr. 8 DS-GVO).

Wenn der Adressat seinen Hauptsitz und/oder eine oder mehrere Niederlassungen in der Union hat, gilt die DS-GVO nach dem Niederlassungsprinzip unabhängig davon, ob die Verarbeitung innerhalb oder außerhalb der EU erfolgt (Art. 3 Abs. 1 DS-GVO).

Wenn der Adressat seinen Hauptsitz außerhalb der Union und auch keine Niederlassung in der Union hat, dann gilt nach dem Marktortprinzip für die Datenverarbeitung von personenbezogenen Daten trotzdem die DS-GVO, soweit der Verantwortliche seine Angebote an Bürger in der EU richtet oder Daten von EU-Bürgern verarbeitet (Art. 3 Abs. 2 DS-GVO).

Pflichten/Anforderungen/Risiken in Bezug auf Daten:

Was ist datenrechtlich geregelt?

– Verbot mit Erlaubnisvorbehalt: Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten und nur ausnahmsweise gestattet, wenn die Voraussetzungen einer der Erlaubnisnormen der DS-GVO greift (Art. 6 Abs. 1 DS-GVO).

– Grundsätze in Art. 5 DS-GVO für die Verarbeitung personenbezogener Daten: Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Vertraulichkeit und Rechenschaftspflicht

– Gewährleistung der Betroffenenrechte in Kapitel III, zentrale Vorschriften für die Pflichten der Verantwortlichen in Kapitel IV und zum Transfer in Drittländer in Kapitel V.

Welche Pflichten werden hinsichtlich der Daten aufgestellt?

– Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DS-GVO) sowie wenn die Daten nicht bei der betroffenen Person selbst erhoben wurden, sondern aus anderen Quellen stammen (Art. 14 DS-GVO)

– Gewährleistung geeigneter technischer und organisatorischer Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit (Art. 24, 25 und 32 DS-GVO)

– Anforderungen an die Auftragsverarbeitung von Daten (Art. 28 DS-GVO)

– Führen eines Verzeichnisses der Verarbeitungstätigkeiten (Art. 30 DS-GVO)

– Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und Benachrichtigung der betroffenen Personen (Art. 33 und 34 DS-GVO)

– Durchführung einer Datenschutz-Folgenabschätzung und vorherige Konsultation der Aufsichtsbehörden (Art. 35 und 36 DS-GVO)

– Benennung eines Datenschutzbeauftragten (Art. 37 bis 39 DS-GVO)

– Vor Übermittlung von Daten in Drittländer außerhalb des EWR sind in der Regel Standardvertragsklauseln mit dem Importeur abzuschließen und ein Transfer Impact Assessment durchzuführen (Art. 44 ff. DS-GVO).

Konzept der Risikoadäquanz: Je wahrscheinlicher oder schwerer das von der Datenverarbeitung ausgehende Risiko ist, desto umfangreicher und höher sind die Pflichten des Verantwortlichen.

Welche Sanktionen sind für Pflichtverletzungen vorgesehen (Risiko)?

– Für die unter Art. 83 Abs. 5 DS-GVO aufgelistete, besonders gravierenden Verstöße sind Bußgelder von bis zu EUR 20.000.000 bzw. bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes vorgesehen (Art. 83 DS-GVO).

– Zudem können zivilrechtliche Schadensersatzansprüche nach Art. 82 DS-GVO drohen (sog. Private Enforcement).

Praktische Hinweise:

Es ist unbedingt das Verbotsprinzip in Art. 6 DS-GVO zu beachten – dabei müssen im Regelfall – Einwilligungen zur Verarbeitung von personenbezogenen Daten eingeholt werden. Auch die Einhaltung der Informationspflicht in Art. 13 DS-GVO sowie die Auskunftspflicht in Art. 15 DS-GVO, und das Recht auf Löschung in Art. 17 DS-GVO ist zentral.

Es muss ein Datenschutzbeauftragter benannt werden (Art. 37 - 39 DS-GVO).

Auch die Ergreifung entsprechender Sicherheitsmaßnahmen nach Art. 32 DS-GVO ist von Relevanz. In der Vergangenheit kam es bereits mehrfach zu sehr hohen Geldbußen, aufgrund unzureichender Sicherung von Daten und damit einhergehender Datenlecks.

Data Governance Act (DGA)



Kurzumriss:

Der Data Governance Act („DGA“) schafft Prozesse, Strukturen und einen Rechtsrahmen für die gemeinsame Nutzung von personenbezogenen und nicht-personenbezogenen Daten. Dadurch soll ein neutraler Zugang zu Daten und die Interoperabilität gesichert sowie Lock-in-Effekte vermieden werden.

Ziel des DGA ist es, die Verfügbarkeit von Daten zur wirtschaftlichen Nutzung, zur gemeinsamen Verwendung und zu Forschungszwecken zu erhöhen, um dem europäischen Markt einen Wettbewerbsvorteil bei datengestützten Innovationen zu verschaffen.

Primärer (datenrechtlicher) Adressat der Regulierung:

Der DGA gilt für öffentliche Stellen sowie Datenvermittlungsdienste und altruistische Organisationen, die in der EU niedergelassen sind, oder ihre Dienste in der EU anbieten. Im letzteren Fall ist ein Vertreter zu benennen.

Pflichten/Anforderungen/Risiken in Bezug auf Daten:

Was ist datenrechtlich geregelt?

Der DGA behandelt drei zentrale Themenfelder:

– Förderung der Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen (Bereitstellung von Daten der öffentlichen Hand, Art. 3 - 9 DGA). Beispiel: finnische Sozial- und Gesundheitsbehörde Findata, bei der Anträge auf Zugang zu Datenquellen wie Sozialversicherungsträgern oder Bevölkerungsregistern gestellt werden können.

– Das Konzept der Datennutzung und -weitergabe durch Datenvermittlungsdienste (Art. 10 - 15 DGA). Diese haben in der heutigen Datenwirtschaft noch kaum Relevanz, die EU hofft aber auf eine Erhöhung der Bedeutung durch Schaffung eines Rechtsrahmens. Vergleichbar ist dies mit einem Kommissionär bei Kommissionsgeschäften nach § 383 HGB. Beispiel: Data Intelligence Hub der Deutschen Telekom AG zur Monetarisierung von Daten.

– Steigerung der Datenverfügbarkeit durch freiwillige Datenspenden aufgrund von Datenaltruismus (Art. 16 - 25 DGA). Die Registrierung als altruistische Organisation kommt nur für unabhängige, nicht-kommerzielle Aktivitäten in Betracht.

Welche Pflichten werden hinsichtlich der Daten aufgestellt?

– Verbot von Ausschließlichkeitsvereinbarungen für Daten im Besitz öffentlicher Stellen (Art. 4 DGA) sowie weitere Pflichten zur Ausgestaltung von Datenlizenzverträgen zwischen öffentlichen Stellen und Privaten (Art. 5 - 6 DGA)

– Anmeldepflicht für Datenvermittlungsdienste (Art. 11 DGA)

– Pflicht zur fairen Preisgestaltung für Datenvermittlungsdienste (Art. 12 Abs. 1 lit. f DGA).

– Eintragungspflicht für datenaltruistische Organisationen (Art. 18 DGA)

– Umfangreiche Transparenzanforderungen und Berichtspflichten für datenaltruistische Organisationen (Art. 20 DGA)

– Umfassende Informationspflichten gegenüber dem Betroffenen bei der Verarbeitung personenbezogener Daten durch datenaltruistische Organisationen (Zweck, Ort der Verarbeitung etc.) (Art. 21 Abs. 1 DGA)

Welche Sanktionen sind für Pflichtverletzungen vorgesehen (Risiko)?

– Die Sanktionen bei Verstößen sind von den EU-Mitgliedstaaten festzulegen. In diesem Zusammenhang ist die für die Einhaltung des DGA national zuständige Behörde befugt, z. B. Geldbußen zu verhängen oder die Erbringung des Datenvermittlungsdienstes auszusetzen (Art. 34 DGA).

Digital Service Act (DSA)

Kurzumriss:

Der Digital Service Act („DAS“) zielt auf ein sichereres und verantwortungsvolleres Online-Umfeld ab. Die Vorschriften sollen ein einheitliches, gemeinsames Regelwerk für die gesamte EU darstellen, die die Grundrechte von Nutzerinnen und Nutzern schützen und Unternehmen der Digitalwirtschaft im gesamten Binnenmarkt Rechtssicherheit bieten sollen. Dadurch soll auch Innovation, Wachstum und Wettbewerbsfähigkeit im EU-Binnenmarkt gefördert werden.

Auch Verbraucherschutz soll hinsichtlich der Regelungen zu Online-Marktplätzen bezweckt werden.

Löst das NetzDG im Wesentlichen ab.

Primärer (datenrechtlicher) Adressat der Regulierung:

Der DSA gilt für alle Vermittlungsdienste, die für Nutzer mit Niederlassungsort oder Sitz in der Union angeboten werden, unabhängig davon, ob der Anbieter der Vermittlungsdienste in der EU oder außerhalb niedergelassen ist (Art. 2 Abs. 1 DSA).

Es erfolgt eine Staffelung, die den Pflichtenkatalog stets erweitert (sehr weiter Anwendungsbereich).

Unterschieden wird zwischen (1) reinen Vermittlungsdiensten, (2) Hostingdiensten, (3) Online-Plattformen (4) Online-Marktplätzen (5) sehr großen Online-Plattformen. Reine Vermittlungsdienste haben die geringsten Verpflichtungen zu erfüllen, und sehr große Online-Plattformen die meisten.

Pflichten/Anforderungen/Risiken in Bezug auf Daten:

Wie bestimmt sich die Einordnung eines Dienstes (Anwendungsbereich)?

- Es muss **immer** ein Dienst der Informationsgesellschaft vorliegen. Ausgeschlossen werden hier vor allem physisch erbrachte Dienste, Telefon und Fax sowie Fernsehen.
- Vermittlungsdienste betreiben reine Durchleitung (abschließende gesetzliche Aufzählung: Caching, Hosting, Suchmaschinen), ohne eine aktive Kenntnis, Rolle oder Kontrolle über die Daten zu haben.
- Hostingdienste als ein Fall von Vermittlungsdiensten speichern Nutzerdaten im Auftrag des Nutzers.
- Online-Plattformen speichern Nutzerdaten im Auftrag des Nutzers und verbreiten diese auch öffentlich. Ausnahme: die öffentliche Verbreitung ist eine unbedeutende, reine Nebenfunktion eines Hostingdienstes oder anderen Dienstes.
- Online-Marktplätze sind Online-Plattformen, bei der zwischen Verbraucher und Unternehmer (B2C) Fernabsatzverträge geschlossen werden.
- Sehr große Online-Plattformen müssen den Schwellenwert von 45 Mio. Nutzern (unique visitors) in der EU überschreiten, und von der Kommission durch Beschluss als solche benannt werden.

Welche Pflichten und Anforderungen werden (gestaffelt nach Anwendungsbereich) hinsichtlich der Daten aufgestellt?

– Zentraler Bezugspunkt einer Vielzahl von Pflichten sind der Umgang mit rechtswidrigen Inhalten = sämtliche Informationen, die nicht im Einklang mit dem Unionsrecht oder dem Recht eines Mitgliedstaats stehen (Art. 3 lit. H DSA).

– Für reine Vermittlungsdienste normiert (1) Art. 4 - 6 DSA Haftungserleichterungen, die sich aus dem Wesen von Vermittlungsdiensten begründen, (2) Art. 9 - 10 DSA Informationspflichten bezüglich Lösch- und Auskunftsanordnungen von Behörden, (3) Art. 11 DSA die Benennung einer zentralen elektronischen Kommunikationsstelle für die Kommunikation mit nationalen Behörden sowie (4) Art. 14 f. DSA Regelungen hinsichtlich der Ausgestaltung von AGB und Transparenzpflichten.

– Für Hostingdiensteanbieter wird zusätzlich normiert (1) die Verpflichtung zur Einrichtung eines Notice-and-action-Systems zur Meldung von rechtswidrigen Inhalten (Art. 16 DSA), (2) Begründungspflichten gegenüber Nutzern bei Löschung potenziell rechtswidriger Inhalte (Art. 17 DSA) sowie (3) eine eigene Meldepflicht bei Verdacht auf bestimmte Straftaten (Art. 18 DSA).

– Für Online-Plattformen wird zusätzlich normiert (1) ein inhaltlich deutlich anspruchsvolleres Beschwerdemanagement- und Streitbeilegungssystem (Art. 21 f. DSA), (2) Sperrpflichten nach vorheriger Warnung u. a. für Nutzer, die häufig rechtswidrige Inhalte einstellen (Art. 23 DSA), (3) Verbot von Dark Patterns (Art. 25 Abs.1 DSA), (4) weitere Transparenzpflichten (Art. 24 und 27 DSA) sowie (5) Ergreifung von Maßnahmen zum Schutz Minderjähriger (Art. 28 DSA).

– Für Online-Marktplätze gelten zusätzlich Verbraucherschutzbestimmungen in den Art. 30 - 32 DSA, mit einer Ausnahme für KMU.

– Für sehr große Online-Plattformen und Online-Suchmaschinen gelten u. a. deutliche Verschärfungen in Art. 34 ff. DSA, der für sie bereits geltenden Regelungen für Online-Plattformen sowie Elemente der Fremd- und Selbstregulierung zur Eindämmung systemischer Risiken (z. B. die Pflicht zur Erstellung von Risikobewertungen etwa bezüglich Verbreitung rechtswidriger Inhalte und Grundrechtsnachteile und die Ergreifung von Maßnahmen).

Welche Sanktionen sind für Pflichtverletzungen vorgesehen (Risiko)?

– Verstöße gegen die Vorschriften des DSA können mit Geldbußen von bis zu 6 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden (vgl. Art. 52 Abs. 3 und Art. 74 Abs. 1 DSA).

Praktische Hinweise:

Die DSA stellt sich als das herausforderndste neue Gesetz in Bezug auf Compliance dar. Allein die Frage, in welche Kategorie der Dienst einzuordnen ist, gestaltet sich im Einzelfall als schwer. Die Erfüllung von Pflichten kann möglicherweise sehr viele Ressourcen in Anspruch nehmen und daher sollte der Dienst nicht aus Sicherheit in eine höhere Kategorie eingeordnet werden. Sobald die Einordnung erfolgt ist, sind die ausführlichen Compliance-Pflichten zu beachten und der Dienst und die Unternehmensorganisation so zu gestalten, dass diese möglichst störungsfrei eingehalten werden („compliance by design“).

AI Act

Kurzumriss:

Der AI Act hat das Ziel, die Verwendung künstlicher Intelligenz zu regulieren. Dabei wird besonderer Wert darauf gelegt, dass KI vertrauenswürdig, sicher, technisch robust, transparent, ethisch, unparteiisch und menschlich kontrollierbar ist.

Der AI Act ist ein präventives, sektorübergreifendes Verbotsgesetz, das den Einsatz von KI in zahlreichen Anwendungsszenarien verbietet oder von technischen, organisatorischen und rechtlichen Anforderungen abhängig macht.

Bezweckt werden soll damit vor allem der Schutz von Grundrechten natürlicher Personen sowie von Urheberrechten.

Im Trilog am 02.02.2024 haben sich viele Vorschriften im Vergleich zu vorherigen Entwürfen noch weiter verschärft.

Zudem wird ein AI Office geschaffen, welches für GPAI-Modelle (wie ChatGPT) als Marktüberwachungsbehörde fungiert.

Primärer (datenrechtlicher) Adressat der Regulierung:

Der AI Act richtet sich überwiegend an Anbieter (Hersteller) und Betreiber von KI-Systemen, umfasst in speziellen Fällen z. B. auch Händler, Bevollmächtigte und Endnutzer.

Als KI System gilt „ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“ Art. 3 Nr. 1 AI Act.

Nach dem Marktortprinzip gilt der AI Act für Anbieter, die KI-Systeme in der Union in Verkehr bringen oder in Betrieb nehmen, Nutzer von KI-Systemen, die sich in der Union befinden sowie Anbieter und Nutzer von KI-Systemen aus Drittländern, deren Systemergebnisse in der Union verwendet werden.

Pflichten/Anforderungen/Risiken in Bezug auf Daten:

Welche wichtigen Transparenzpflichten werden in Bezug auf KI-Systeme aufgestellt, die mit natürlichen Personen interagieren?

– Anbieter von KI-Systemen (Art. 3 Nr. 3 AI Act) müssen bei Verwendung eines KI-Systems gegenüber natürlichen Personen darauf hinweisen, dass mit einem KI-System interagiert wird (Art. 50 AI Act).

– Anbieter von KI-Systemen (Art. 3 Nr. 3 AI Act), die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen, stellen sicher, dass das Output des KI-Systems erkennbar als solches, in maschinenlesbarer Art gekennzeichnet ist (etwa durch Wasserzeichen, Metadaten, kryptographische Methoden, digitale Fingerabdrücke, etc.).

– Betreiber von KI-Systemen (Art. 3 Nr. 4 AI Act) müssen die davon betroffene natürliche Person über den Einsatz von Emotionserkennungssoftware sowie biometrischer Kategorisierungssysteme informieren.

– Betreiber eines KI-Systems (Art. 3 Nr. 4 AI Act), das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die ein Deepfake sind, müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden.

Welche wichtigen zusätzlichen Pflichten gibt es für GPAI-Modelle wie ChatGPT?

– GPAI-Modelle = KI-System mit allgemeinem Verwendungszweck im Sinne des Art. 3 Nr. 66 AI Act, mithin ein KI-Modell, das „[…] in der Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen".

– Pflichten des Art. 53 AI Act: u. A. Dokumentation des Modells; Zurverfügungstellung der Dokumentation für Anbieter von KI-Systemen, die GPAI-Modell in ihre KI-Systeme integrieren wollen; Veröffentlichung der der für das Training des KI-Modells verwendeten Inhalte.

– Zusätzliche Anforderungen für Anbieter von Modellen mit systemischen Risiken (zum Begriff siehe Art. 3 Nr. 65 AI Act) nach Art. 55 AI Act: u. a. Durchführung und Dokumentation von Angriffstests, Risikobewertung und Risikominderung, Gewährleistung eines angemessenen Maßes an Cybersicherheit).

Welche KI-Systeme sind u. a. verboten?

– Social-Scoring-Systeme (Art. 5 lit. c AI Act), Profiling in der Strafverfolgung (Art. 5 lit. d. AI Act), Datenbank-KI-Systeme zur Gesichtserkennung (Art. 5 lit. e AI Act), Emotionserkennungssysteme in Schulen und Arbeitsplätzen (Art. 5 lit. f AI Act)

– KI-Systeme, die manipulative Techniken oder persönliche Schwächen ausnutzen, um zu einem schädigenden Verhalten zu bewegen (Art. 5 lit. a, b AI Act)

Welche wichtigen Pflichten werden für Hochrisiko-KI-Systeme aufgestellt?

– Die Einstufung als Hochrisiko-KI-System orientiert sich an (1) Produktart, u. a. Anwendung von KI in Maschinen, Spielzeug, Medizinprodukten und/oder (2) Hochrisiko-Bereiche wie biometrische Daten, kritische Infrastruktur, Beschäftigung/Personalmanagement, Strafverfolgung, Rechtspflege, demokratische Prozesse, etc..

– Hochrisiko-KI-Systeme müssen ein Risikomanagementsystem einrichten, anwenden, dokumentieren und aufrechterhalten (Art. 9 AI Act). Das Hochrisiko-KI-Systems muss die automatische Protokollierung von Ereignissen während des Lebenszyklus des Systems ermöglichen (Art. 12 AI Act).

– Strenge Anforderungen an Trainingsdaten: Daten müssen im Hinblick auf die Zweckbestimmung des KI-Systems relevant, hinreichend repräsentativ, und so weit wie möglich fehlerfrei und vollständig sein (Art. 10 AI Act).

– Dem Nutzer muss eine Interpretation des Outputs ermöglicht sein (Art. 13 AI Act). Zentrale technische Herausforderung, da die meisten KI-Systeme heutzutage noch eine „Black Box" sind; ihr Ergebnis also nicht erklären können.

– Menschlicher Anwender muss in der Lage sein, das System zu überwachen (Art. 14 AI Act); Konformitätsbewertung vor dem Inverkehrbringen (Art. 19, 44 AI Act)

Welche Sanktionen sind für Pflichtverletzungen vorgesehen (Risiko)?

– Bei Verstößen gegen Missachtung des Verbots der in Art. 5 genannten KI-Praktiken drohen Bußgelder von bis zu EUR 35 Millionen/ bis zu 7 % des weltweiten Jahresumsatzes.

– Im Falle von KI-Modellen mit allgemeinem Verwendungszweck drohen Geldbußen von bis zu EUR 15 Mio./ 3 % des weltweiten Jahresumsatzes.

Open Data Directive



Kurzumriss:

Die Open Data Directive hat sich zum Ziel gesetzt, die Verfügbarkeit und den Fluss von Daten im Besitz von öffentlich-rechtlichen Körperschaften für kommerzielle und nichtkommerzielle Zwecke zu erhöhen. Es sollen Zugriffsmöglichkeiten verbessert werden, indem die unterschiedlichen Bedingungen und Verfahren der Mitgliedstaaten zur Nutzung von Informationsquellen des öffentlichen Sektors vereinheitlicht werden.

Primärer (datenrechtlicher) Adressat der Regulierung:

Adressat sind öffentlich-rechtliche Körperschaften innerhalb der EU, auch etwa Universitäten in Bezug auf Forschungsdaten.

Kulturelle Institutionen wie Museen, und der öffentlich-rechtliche Rundfunk sind allerdings ausgenommen.

Es ist zu beachten, dass nur solche Daten vom Anwendungsbereich erfasst sind, die bereits auf Basis von anderen Rechtsakten für öffentlich verfügbar erklärt wurden, und dass Daten, die geistiges Eigentum Dritter betreffen, ausgenommen sind. Sensible (u. a. sicherheitsrelevante) Daten sind ebenfalls ausgenommen.

Primär zielt die Open Data Directive daher auf die Vereinfachung des „wie“ in Bezug auf Datenverfügbarkeit öffentlich-rechtlicher Körperschaften ab, nicht auf das „ob“.

Pflichten/Anforderungen in Bezug auf Daten:

– Öffentlich-rechtliche Körperschaften, die vorher „sui generis“-Rechte in Bezug auf Datenbanken o. ä. hatten, dürfen sich auf diese nach Inkrafttreten nicht länger berufen.

– Art. 4 Open Data Directive bestimmt die Modalitäten der Datenbereitstellung: u. a. Fristen zur Bereitstellung für die Körperschaft, Begründungs- und Rechtsbehelfsbelehrungspflichten bei Negativbescheidung.

– Art. 5 Open Data Directive verpflichtet die Körperschaften zur möglichst barrierefreien Bereitstellung von Daten, soweit möglich über das Internet.

– Art. 6 Open Data Directive regelt Modalitäten bezüglich Gebühren, u. a. dürfen nur notwendige Aufwendungen für die Datenweitergabe geltend gemacht werden. Es bestehen Ausnahmen u. a. für Bibliotheken und Körperschaften, die sich über Gebühren finanzieren.

– Es dürfen keine zusätzlichen Bedingungen für die Datennutzung auferlegt (Art. 8 Open Data Directive) und keine Ausschließlichkeitsvereinbarungen geschlossen werden (Art. 12 Open Data Directive).

e-Privacy-Verordnung

Kurzumriss:

Der **Entwurf der e-Privacy-Verordnung** ist ein Gesetzesvorschlag zur Achtung der Privatsphäre und dem Schutz personenbezogener Daten in der elektronischen Kommunikation. Im Schwerpunkt regelt die Verordnung die Vertraulichkeit der Kommunikation (Fernmeldegeheimnis) sowie die Verarbeitung von Kommunikationsdaten.

Es sollen spezifische Regelungen im Bereich der elektronischen Kommunikation umgesetzt werden, welche die DS-GVO mit ihrem technologieneutralen Ansatz nicht erfüllen kann.

Die e-Privacy-Verordnung ist Stand Juni 2024 weiterhin nicht beschlossen, und das weitere Vorgehen bleibt unklar. Soweit diese in Kraft tritt, wird sie aber ähnlich wie die DS-GVO umfassende Handlungspflichten für Plattformbetreiber begründen.

Primärer (datenrechtlicher) Adressat der Regulierung:

Unternehmen der Digitalwirtschaft, v. a. Website- und Software-Anbieter.

Pflichten/Anforderungen/Risiken in Bezug auf Daten:

– Anbieter sollen verpflichtet werden, die Daten nach dem Stand der Technik zu sichern und vor unbefugtem Zugriff zu schützen.

– Es soll der Handel mit Daten durch die Hintertüre verboten werden (Backdoors).

– Das räumliche Tracking durch Programme, die nicht aktiv genutzt werden (unwissentliche Anfertigung von Bewegungsprofilen), soll verboten werden.

– Es soll keine Verarbeitung von Daten ohne Einverständnis des Nutzers erfolgen. Diese Verpflichtung soll durch die Verordnung auf Anbieter der Online-Kommunikation ausgeweitet werden und ohne Einwilligung zur Speicherung soll keine Verarbeitung erfolgen.

– In allen Software- und Geräteeinstellungen soll standardmäßig die datenschutzfreundlichere Variante eingestellt sein (Privacy-by-default).

– Schutz der Privatsphäre: Anzeige von Rufnummern, Endnutzerverzeichnis, Direktwerbung mittels elektronischer Kommunikation und die Aufsicht

– Verweise auf die Regelung zu den Bußgeldvorschriften der DS-GVO geplant (Art. 23 e-Privacy Verordnung-E)

Free-Flow-of-Data-Verordnung

Kurzumriss:

Die Free-Flow-of-Data-Verordnung hat zum Ziel, Hindernisse für den freien Verkehr nicht-personenbezogener Daten innerhalb der Europäischen Union zu beseitigen, um eine wettbewerbsfähige Datenwirtschaft im digitalen Binnenmarkt herzustellen.

Dadurch soll die Niederlassungsfreiheit und Dienstleistungsfreiheit (AEUV) von Datenverarbeitungsdiensten geschützt werden, die davor durch mögliche nationale oder regionale Anforderungen tangiert sein könnte.

Auch privatrechtliche Beschränkungen sollen reduziert werden.

Primärer (datenrechtlicher) Adressat der Regulierung:

Adressat der Verordnung sind Dienstleister, die für Nutzer innerhalb der Europäischen Union elektronische (nicht personenbezogene) Daten verarbeiten sowie natürliche und juristische Personen, die Daten für ihren eigenen Bedarf verarbeiten.

Primär geht es um die Verbesserung der Verarbeitung und Übertragung nicht personenbezogener Daten über nationale Grenzen hinweg.

Pflichten/Anforderungen/Risiken in Bezug auf Daten:

– Verbot nationaler Datenlokalisierungsauflagen, sofern diese nicht aus Gründen der öffentlichen Sicherheit unter Achtung des Grundes der Verhältnismäßigkeit gerechtfertigt sind (Art. 4 Abs. 1 Free-Flow-of-Data-Verordnung).

– Verfügbarkeit von Daten für zuständige Behörden, damit nationale Verwaltungs- und Justizbehörden der Zugang zu den Daten ermöglicht wird, auch wenn sich diese in einem anderen Mitgliedstaat befinden (Art. 5 Abs. 1 Free-Flow-of-Data-Verordnung).

– Einfacherer Wechsel der Cloud Service Provider für professionelle Anwender (sog. Datenportabilität), da der Standort und das Angebot von Diensten nicht mehr auf Mitgliedstaaten beschränkt werden kann.

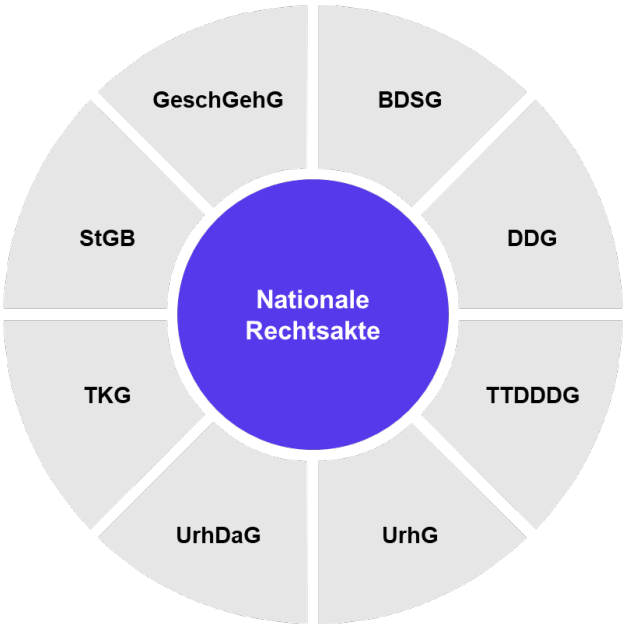
– Unternehmen sollen Verhaltensregeln erstellen (Code of Conduct), die die Grundsätze der Transparenz und der Interoperabilität sicherstellen (Art. 6 Free-Flow-of-Data-Verordnung).

Nationale Rechtsvorschriften

Einfühlung

Nicht nur auf europäischer Ebene gilt es Regulierungen im Hinblick auf das Wirtschaftsgut „Daten“ zu beachten. Auch auf nationaler Ebene sind bestimmte Gesetze im Zusammenhang mit der Datenwirtschaft zu beachten. Diese können in ihren Anforderungen und Schwerpunkten erheblich variieren, oder auch nur fragmentierte Regelungen zu Daten enthalten.

Überblick über die wichtigsten nationalen Rechtsakte



Die nationalen Rechtsvorschriften im Einzelnen

Legende

	Gesetz/Vorschriften betreffen nicht-personenbezogene Daten
	Gesetz/Vorschriften betreffen personenbezogene Daten
§	Datum des Inkrafttretens des Gesetzes

GeschGehG

Kurzumriss:

Das Gesetz zum Schutz von Geschäftsgeheimnissen („GeschGehG“) geht auf europarechtliche Vorgaben zurück. Es hat zum Ziel, einen einheitlichen zivilrechtlichen Mindestschutz von Geschäftsgeheimnissen sicherzustellen.

Hintergrund ist, dass sich Unternehmen – u. a. aufgrund der Globalisierung, des zunehmenden Outsourcings und des verstärkten Einsatzes von IT-Systemen – zunehmend unlauteren Praktiken ausgesetzt sehen, die auf eine rechtswidrige Aneignung von Geschäftsgeheimnissen abzielen (Wirtschaftsspionage, Diebstahl, unbefugtes Kopieren, Verletzung von Geheimhaltungspflichten, o. ä.).

Primärer (datenrechtlicher) Adressat der Regulierung:

Dient dem Schutz von Inhabern von Geschäftsgeheimnissen: jede natürliche oder juristische Person mit rechtmäßiger Kontrolle über ein Geschäftsgeheimnis (§ 2 Nr. 2 GeschGehG).

Soll Verletzer von Geschäftsgeheimnissen durch zivilrechtliche Klagemöglichkeiten und Strafrechtsvorschriften sanktionieren.

Geschäftsgeheimnisse sind nach § 2 Nr. 1 GeschGehG eine Information,

a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und

b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Pflichten/Anforderungen/Risiken in Bezug auf Daten:

Welche Arten von Daten kommen für Geschäftsgeheimnisse in Frage?

– „Informationsbegriff“ ist sehr weit zu verstehen – jegliches Know-How, wie Herstellungsverfahren, Kunden- und Lieferantenlisten, Kosteninformationen, Geschäftsstrategien, Unternehmensdaten, Marktanalysen, Prototypen, Formeln und Rezepte.

– Die Information muss einen wirtschaftlichen Wert haben, und zwar weil sie nicht offenkundig bekannt ist. Belanglose Informationen scheiden aus, auch wenn sie an sich geheim sind.

– Es müssen angemessene Geheimhaltungsmaßnahmen getroffen werden. Gefordert wird ein aktives Tun (Obliegenheit).

Wann wird ein Geschäftsgeheimnis verletzt und welche Ansprüche und Sanktionen gibt es?

– Rechtsverletzer: jede natürliche oder juristische Person, die entgegen den Handlungsverboten in § 4 GeschGehG (u. a. unbefugter Zugang, Kopieren) ein Geschäftsgeheimnis erlangt, nutzt oder offenlegt. **Ausnahmen** hierzu in § 5 GeschGehG (sog. Whisteblower-Paragraph)

– §§ 6 - 8 GeschGehG: Auskunfts-, Beseitigungs- und Unterlassungsanspruch. Ein Verschulden wird nicht vorausgesetzt, nach § 9 GeschGehG gibt es allerdings eine Unverhältnismäßigkeitseinrede

– § 10 GeschGehG: Schadensersatzanspruch in Geld (bei Schuldhaftigkeit)

– § 13 GeschGehG: Bereicherungsrechtlicher Anspruch

– § 23 GeschGehG: Straftatbestand

Praktische Hinweise:

Zunächst muss identifiziert werden, welche Informationen nach wirtschaftlichen Gesichtspunkten schutzwürdig sind. Dann sollten die schutzbedürftigen Informationen nach Schutzbedürftigkeit klassifiziert werden. Im Anschluss daran muss ein Schutzkonzept erarbeitet und im Unternehmen umgesetzt, sowie deren Wirksamkeit regelmäßig überprüft werden.

Als Schutzmaßnahmen kommen unter anderem in Betracht:

– Need-to-Know-Prinzip: Jedem Arbeitgeber werden nur die Informationen zur Verfügung gestellt, die er zur Erledigung seiner Aufgaben braucht.

– auf Vertraulichkeitsvereinbarungen bestehen

– Nutzung privater elektronischer Geräte und Mitnahme von beruflichen Unterlagen untersagen

– sichere IT-Infrastruktur betreiben

– Protokollierung von Zugriffen auf physische und elektronische Daten

Wichtig ist, dass Schutzmaßnahmen ergriffen werden, da sonst die Geltendmachung von Ansprüchen verwehrt sein könnte. Die Intensität der ergriffenen Maßnahmen kommt dabei auf die Vertraulichkeit der konkreten Geschäftsgeheimnisse an. Eine Rolle spielt auch die Verhältnismäßigkeit der Maßnahmenergreifung: Wenn zur wirtschaftlichen Funktionsfähigkeit des Unternehmens das „Need-to-know“-Prinzip nicht umgesetzt werden kann, wird auch in aller Regel nicht erwartet, dass dieses umgesetzt wird.

BDSG

Kurzumriss:

Das Bundesdatenschutzgesetz („BDSG“) orientiert sich in seiner Grundstruktur an der DS-GVO und soll diese ergänzen. Es setzt die Regelungsaufträge aus der DS-GVO an die Mitgliedstaaten um.

Es soll insbesondere für die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten öffentlicher Stellen des Bundes Anwendung finden, die außerhalb des Anwendungsbereichs des Unionsrechts liegen.

Das Bundesdatenschutzgesetz (BDSG) legt ferner Verpflichtungen für nicht-öffentliche Stellen fest, insbesondere in Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten sowie für spezielle Verarbeitungssituationen, in denen die Datenschutz-Grundverordnung (DS-GVO) Öffnungsklauseln zugunsten des nationalen Rechts enthält.

Primärer (datenrechtlicher) Adressat der Regulierung:

Das BDSG adressiert primär öffentliche Stellen des Bundes und der Bundesländer, sofern sie Bundesrecht ausführen.

Für nicht-öffentliche Stellen gilt das BDSG, sofern der Verantwortliche oder Auftragsverarbeiter personenbezogene Daten im Inland verarbeiten, oder die Verarbeitung in einer inländischen Niederlassung erfolgt. Das BDSG findet auch Anwendung für nicht-öffentliche Stellen ohne Niederlassung in einem Mitgliedstaat der EU oder einem Vertragsstaat des EWR, sofern sie in den Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO) fallen. Die Verarbeitung muss ganz oder teilweise automatisiert erfolgen oder nicht automatisiert, wenn die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Eine Ausnahme besteht bei der Verarbeitung durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

Pflichten/Anforderungen in Bezug auf Daten für nichtöffentliche Stellen:

– Videoüberwachung öffentlich zugänglicher Räume nur unten den in § 4 BDSG genannten Voraussetzungen zulässig; Beachte: Vorrang der DS-GVO in deren Anwendungsbereich

– Besondere Anforderungen für die Datenverarbeitung im Beschäftigungsverhältnis, § 26 BDSG: u. a. besondere Voraussetzungen für die Einwilligung des Beschäftigten in die Verarbeitung seiner personenbezogenen Daten

– Einhaltung der Voraussetzungen des § 31 BDSG bei Scoring

Konsequenzen bei Verstoß gegen die Vorschriften:

– Schadensersatz-/Entschädigungsansprüche nach § 83 BDSG

– Bußgelder (§ 43 BDSG) und strafrechtliche Konsequenzen (§ 42 BDSG)

Praktische Hinweise:

Im Rahmen des BDSG wird insbesondere auf die besonderen Voraussetzungen des § 26 Abs. 2 BDSG im Rahmen der Einwilligung Beschäftigter zu achten sein und auf die Voraussetzungen des § 31 BDSG beim Scoring.

DDG

Kurzumriss:

Das Digitale-Dienste-Gesetz („DDG“) löst das Telemediengesetz (TMG) ab, setzt die Regelungsaufträge des DSA (Digital Services Act) um und passt den nationalen Rechtsrahmen zur effektiven Umsetzung des DSA entsprechend an.

Hierbei benennt das DDG die Bundesnetzagentur als zuständige Stelle für die Durchsetzung des DSA und regelt die Konsequenzen für Verstöße gegen den DSA. Im Übrigen werden die Regelungen des TMG weitestgehend identisch übernommen, die auch datenrechtlich relevante Regelungen enthalten.

Primärer (datenrechtlicher) Adressat der Regulierung:

Primärer Adressat der datenrechtlichen Regelungen sind Anbieter digitaler Dienste, worunter eine Dienstleistung der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung, zu verstehen ist.

Der Anwendungsbereich umfasst Diensteanbieter, die in Deutschland niedergelassen sind, auch wenn sie ihre Dienstleistungen in einem anderen Mitgliedstaat der Europäischen Union erbringen, soweit in diesem Fall nicht der DSA direkt gilt.

Pflichten/Anforderungen in Bezug auf Daten:

– Impressumspflicht nach § 5 DDG

– Besondere Transparenzpflichten im Hinblick auf Werbung nach § 6 DDG: u. a. Erkennbarkeit von Angeboten zur Verkaufsförderung, Preisnachlässe, Zugaben und Geschenke als solche; Preisausschreiben oder Gewinnspiele mit Werbecharakter müssen klar als solche erkennbar sein.

– Anspruch des Inhabers von geistigen Eigentumsrechten auf Sperrung der Nutzung von Informationen bei Rechtsverletzung, § 8 DDG.

– Pflichten für Videosharingplattform-Anbieter (zum Begriff § 1 Abs. 4 Nr. 9 DDG) nach § 11 DDG: insb. vertragliche Nutzungsverbote mit Nutzern vereinbaren, dass diese auf der Videosharingplattform keine unzulässige Werbung, bspw. in Bezug auf Tabakerzeugnisse oder verschreibungspflichtige Arzneimittel, verbreiten dürfen.

Konsequenzen bei Verstoß gegen die Pflichten:

– Bußgelder nach § 33 DDG

Praktische Hinweise:

Insbesondere Aktualisierung des Impressums von TMG auf DDG und bei Anbietern von audiovisuellen Mediendiensten die Angabe des Mitgliedstaats, der für sie Sitzland ist oder als Sitzland gilt sowie die zuständigen Regulierungs- und Aufsichtsbehörden. Ansonsten ergeben sich hinsichtlich der Impressumspflicht keine Neuerungen durch das DDG.

Im Hinblick auf die Tranparenzpflichten nach § 6 DDG ergeben sich keine weitreichenden Änderungen im Vergleich zur Rechtslage nach dem TMG. Es wurden in Absatz 3 und 4 lediglich spezielle Vorschriften für Videosharingplattform-Anbieter eingeführt.

Ein dem § 8 DDG vergleichbarer Anspruch fand sich im TMG noch nicht, weshalb es die diesbezüglichen Voraussetzungen zu schaffen gilt.

Die Pflichten für Videosharingplattform-Anbieter nach § 11 DDG wurden weitestgehend neu eingeführt.

TTDDG

Kurzumriss:

In dem Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten („TDDDG“) (vormals TTDSG) wurden die Datenschutzbestimmungen des TMG (nunmehr DDG) und TKG, einschließlich der Bestimmungen zum Schutz des Fernmeldegeheimnisses an die DS-GVO angepasst und zusammengeführt. Zudem wurden die Regelungen zum Schutz der Privatsphäre in Endeinrichtungen der e-Privacy-Richtlinie der EU in nationales Recht umgesetzt.

Die Vorschriften betreffen den Datenschutz bei Telekommunikations- und digitalen Diensten. Sie umfassen Anforderungen an die Privatsphäre in Bezug auf ankommende Verbindungen, Rufnummernunterdrückung, -anzeige und automatische Anrufweiterleitung sowie den Schutz der Privatsphäre bei Endgeräten.

Primärer (datenrechtlicher) Adressat der Regulierung:

Primäre Adressaten des TDDDG sind Anbieter digitaler Dienste (§ 2 Abs. 2 Nr. 1 TDDDG) und Telekommunikationsdiensteanbieter, die in Deutschland eine Niederlassung haben oder Dienstleistungen erbringen oder daran mitwirken oder Waren auf dem Markt bereitstellen.

Pflichten/Anforderungen in Bezug auf Daten:

– Es dürfen nur die in § 9 Nr. 1 - 5 TDDDG genannten Verkehrsdaten von Anbietern öffentlich zugänglicher Telekommunikationsdienste sowie von natürlichen und juristischen Personen, die an der Erbringung solcher Dienste mitwirken, erhoben werden, soweit dies zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen erforderlich ist.

– Pflichten im Hinblick auf Standortdaten nach § 13 TDDDG

– Regelungen zur Rufnummeranzeige und -unterdrückung nach § 15 TDDDG: u. a. Anbieter von Sprachkommunikationsdiensten müssen Endnutzern die Möglichkeit zur Rufnummerunterdrückung unentgeltlich anbieten; gleichzeitig sollten angerufene Endnutzer die Option haben, eingehende Anrufe mit unterdrückter Rufnummer abzulehnen; bei Werbeanrufen darf die Rufnummer nicht unterdrückt werden.

– Datenschutzpflichten bei digitalen Diensten: u. a. technische und organisatorische Vorkehrungen, wie die Möglichkeit der Nutzung und Bezahlung von digitalen Diensten anonym oder unter Pseudonym (§ 19 TDDDG); Verarbeitung personenbezogener Daten Minderjähriger (§ 20 TDDDG); Regelungen zur Auskunft über Bestandsdaten (§§ 21, 22 TDDDG)

– Datenschutzpflichten bei Endeinrichtungen (§ 2 Abs. 2 Nr. 6 TDDDG) nach §§ 25, 16 TDDDG: u. a. Einwilligungserfordernis für Cookies und ähnliche Technologien

UrhG



Kurzumriss:

Das Gesetz über Urheberrecht und verwandte Schutzrechte („UrhG“) regelt primär Rechte des Urhebers eines Werkes der Literatur, Wissenschaft und Kunst. Vordergründig handelt es sich demnach nicht um ein datenrechtliches Regelwerk, allerdings sind auch im UrhG einige relevante Pflichten zu finden.

Beachtlich sind insbesondere die Vorschriften zu Datenbankherstellern, welche ebenjenen ein Schutzrecht zugunsten der gesamten oder einem nach Art oder Umfang wesentlichen Teil der Datenbank einräumen.

Primärer (datenrechtlicher) Adressat der Regulierung:

Zur Einhaltung der Schutzvorschriften zugunsten von Datenbankherstellern verpflichtet sind sämtliche natürliche und juristische Personen des Privatrechts und des Öffentlichen Rechts.

Geschützt sind deutsche Staatsangehörige, sowie Staatsangehörige eines anderen Mitgliedstaates der EU. Zudem unterfallen dem Schutzbereich juristische Personen, die in Deutschland oder einem anderen Mitgliedstaat der EU gegründet wurden, oder deren Hauptverwaltung oder Hauptniederlassung sich in einem der Staaten befindet. Im Übrigen sind auch juristische Personen, deren satzungsmäßiger Sitz sich im Gebiet eines dieser Staaten befindet und ihre Tätigkeit eine tatsächliche Verbindung zur deutschen Wirtschaft oder zur Wirtschaft eines dieser Staaten aufweist, umfasst.

Pflichten/Anforderungen in Bezug auf Daten:

– Kein Verstoß gegen das Schutzrecht des Datenbankherstellers (zum Begriff § 87a UrhG)

Konsequenzen bei Verstoß gegen Schutzrecht:

– Anspruch auf Unterlassung/Beseitigung/Schadensersatz

– Strafrechtliche Konsequenzen sowie Bußgelder

UrhDaG

Kurzumriss:

Das Gesetz über die urheberrechtliche Verantwortlichkeit von Diensteanbietern für das Teilen von Online-Inhalten („UrhDaG“) regelt die Verantwortlichkeit eines Diensteanbieters (§ 2 UrhDaG), welcher Werke öffentlich wiedergibt, indem er der Öffentlichkeit Zugang zu urheberrechtlich geschützten Werken verschafft, die von Nutzern des Dienstes hochgeladen worden sind.

Ergreift der Diensteanbieter die in dem UrhDaG genannten Maßnahmen, ist er für die öffentliche Widergabe des geschützten Werkes urheberrechtlich nicht verantwortlich.

Primärer (datenrechtlicher) Adressat der Regulierung:

Primärer Adressat der Verpflichtungen sind Diensteanbieter (§ 2 UrhDaG). Dies sind Anbieter von Dienstleistungen der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung, die zudem die Voraussetzungen des § 2 Nr. 1 - 4 UrhDaG erfüllt.

Räumlich beschränkt sich der Anwendungsbereich der Vorschrift auf das Inland.

Pflichten/Anforderungen für Diensteanbieter Bezug auf Daten:

– Verpflichtung zur bestmöglichen Anstrengung zum Erwerb vertraglicher Nutzungsrechte für die öffentliche Wiedergabe urheberrechtlich geschützter Werke, § 4 UrhDaG

– Verpflichtung zur Blockierung von Inhalten, §§ 7 - 11 UrhDaG

– Vergütungspflicht nach § 12 Abs. 1 UrhDaG gegenüber dem Urheber bei mutmaßlich erbauten Nutzungen nach den §§ 9 - 11 UrhDaG

– Bereitstellung eines wirksamen, kostenfreien und zügigen Beschwerdeverfahrens über die Blockierung und über die öffentliche Wiedergabe von geschützten Werken, § 14 UrhDaG

Konsequenzen bei Verstoß gegen die Verpflichtungen:

– Vollständige urheberrechtliche Verantwortlichkeit des Diensteanbieters für die unerlaubte öffentliche Wiedergabe urheberrechtlich geschützter Werke

TKG

Kurzumriss:

Das Telekommunikationsgesetz („TKG“) soll den Wettbewerb im Bereich der Telekommunikation fördern und zum Aufbau leistungsfähiger Telekommunikationsinfrastrukturen führen, um flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten.

Es legt klare Anforderungen und Verpflichtungen für Anbieter öffentlich zugänglicher Telekommunikationsdienste fest, um die Sicherheit und den Schutz personenbezogener Daten zu gewährleisten.

Primärer (datenrechtlicher) Adressat der Regulierung:

Adressat der Regulierung sind primär alle Unternehmen oder Personen, die Telekommunikationsnetze oder Telekommunikationsanlagen betrieben oder Telekommunikationsdienste in Deutschland erbringen.

Pflichten/Anforderungen in Bezug auf Daten für Betreiber öffentlicher Telekommunikationsnetze (§ 3 Nr. 7, 42 TKG):

– Meldepflicht nach § 5 TKG für Betreiber gewerblicher öffentlicher Telekommunikationsnetze

– Verpflichtung zum Jahresfinanzbericht für die unter § 6 Abs. 1 TKG fallenden Unternehmen

– Schnittstellenbeschreibungen nach § 74 TKG

Pflichten/Anforderungen in Bezug auf Daten für Unternehmen mit beträchtlicher Marktmacht:

– Bundesnetzagentur kann Unternehmen mit beträchtlicher Marktmacht Verpflichtungen nach §§ 24 - 30, 38 oder 49 TKG auferlegen

– Missbrauchsverbot gegenüber Endnutzern oder anderen Unternehmen, § 37, 50 TKG

Pflichten/Anforderungen in Bezug auf Daten für Anbieter öffentlich zugänglicher Telekommunikationsdienste (§ 3 Nr. 1, 44 TKG):

– Informationspflichten für Anbieter von Internetzugangsdiensten und öffentlich zugänglichen interpersonellen Telekommunikationsdiensten, § 52 TKG

– Vertragsrechtliche Anforderungen gegenüber Verbrauchern, § 54 - 57 TKG: u. a. Informationspflichten, Vertragszusammenfassung, Kündigung nach stillschweigender Vertragsverlängerung, Vertragsänderung

– Verpflichtung zur Beseitigung von Störungen auf Verlangen des Verbrauchers, § 58 TKG

– Anforderungen an die Verbindungspreisberechnung nach § 63 TKG für Anbieter öffentlich zugänglicher nummerngebundener interpersoneller Telekommunikationsdienste und Anbieter von Internetzugangsdiensten

– Anspruch des Endnutzers auf Einzelverbindungsnachweis nach § 65 TKG gegenüber Anbietern öffentlich zugänglicher nummerngebundener interpersoneller Telekommunikationsdienste und von Anbietern von Internetzugangsdiensten

– Benachrichtigungspflicht von Anbietern öffentlich zugänglicher Telekommunikationsdienste im Falle der Verletzung personenbezogener Daten an die Bundesnetzagentur, § 169 TKG

– Verpflichtung zur Speicherung von Verkehrsdaten, zur Verwendung der Daten und zur Datensicherheit für Anbieter öffentlich zugänglicher Telekommunikationsdienste, bei denen es sich nicht um nummernunabhängige interpersonelle Telekommunikationsdienste handelt (§§ 175-181 TKG)

Datenbezogene Verpflichtungen für Anbieter öffentlich zugänglicher Telekommunikationsdienste und Betreiber öffentlicher Telekommunikationsnetze:

– Diskriminierungsverbot gegenüber Endnutzern; Berücksichtigung von Interessen von Endnutzern mit Behinderung, § 51 TKG

– Regelungen zum Anbieterwechsel und zur Rufnummermitnahme, § 59 TKG

Konsequenzen bei Verstoß gegen die Verpflichtungen:

– Abwehr und Schadensersatzansprüche nach § 69 TKG

– Bußgelder nach § 228 TKG

StGB

Kurzumriss:

Auch das Strafgesetzbuch („StGB“) enthält in zahlreichen Vorschriften datenrechtliche Regelungen.

Primärer (datenrechtlicher) Adressat der Regulierung:

Das StGB gilt in der Regel für Taten, die im Inland begangen werden (§ 3 StGB).

Relevante datenrechtliche Vorschriften:

– § 126a StGB: Gefährdendes Verbreiten personenbezogener Daten

– § 202a StGB: Ausspähen von Daten

– § 202b StGB: Abfangen von Daten

– § 202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten

– §202d StGB: Datenhehlerei

– § 238 Abs. 1 Nr. 3 StGB: Nachstellung, indem wiederholt unter missbräuchlicher Verwendung von personenbezogenen Daten dieser Person a) Bestellungen von Waren oder Dienstleistungen für sie aufgibt oder b) Dritte veranlasst, Kontakt mit ihr aufzunehmen.

– § 263a StGB: Computerbetrug

– § 268 StGB: Fälschung technischer Aufzeichnungen

– § 269 StGB: Fälschung beweiserheblicher Daten

– § 270 StGB: Täuschung im Rechtsverkehr bei Datenverarbeitung

– § 274 Abs. 2 Nr. 2 StGB: Urkundenunterdrückung, Veränderung einer Grenzbezeichnung

– § 303a StGB: Datenveränderung

– § 303b StGB: Computersabotage

Konsequenzen bei Verstoß gegen die Vorschriften

Geldstrafe oder Freiheitsstrafe bis zu 5 Jahren

info@noerr.com
noerr.com