

Neuerungen durch die Datenschutzgrundverordnung

26. April 2017
World IP Day 2017

Mag. Georg LECHNER

Hinweis 1

Die nachfolgenden Informationen geben einen allgemeinen Überblick. Daraus getroffene Ableitungen geben ausschließlich die persönliche Meinung des Vortragenden wieder.

Hinweis 2

- Die nachfolgenden Informationen basieren auf der deutschen Sprachfassung der DSGVO
- Da die Verhandlungen primär auf Basis englischsprachiger Dokumente geführt wurden, wird empfohlen, bei Auslegungsfragen auf die englische Sprachfassung der DSGVO zurückzugreifen.
- Es wird vermutlich eine Berichtigung der deutschen Sprachfassung geben

Das „Datenschutzpaket“

- Datenschutz-Grundverordnung (VO (EU) Nr. 2016/679)
- Richtlinie für den Bereich Justiz und Inneres (RL Nr. 2016/680)
- Anwendbarkeit: **25.05.2018**

Datenschutz-Grundverordnung

- Grundlage des allgemeinen Datenschutzes in Europa, gilt nur für natürliche Personen
- „hinkende Verordnung“ – Umsetzungsmaßnahmen erforderlich
- Zielsetzungen:
 - einheitlicher Rechtsschutz
 - einheitliche Regeln für Datenverarbeitung, Abbau von Handelshindernissen
 - starker und einheitlicher Vollzug

Datenschutz-Grundverordnung

Vergleich mit DS-RL

Datenschutzrichtlinie 95/46/EG

- 72 Erwägungsgründe
- 34 Artikel
- Umsetzung in nationales Recht
- Text offen und allgemein gehalten

Datenschutz-Grundverordnung

- 173 Erwägungsgründe
- 99 Artikel
- tlw. Konkretisierung durch nationale Gesetze erforderlich
- Text tlw. sehr detailliert

Richtlinie für den Bereich Justiz und Inneres

- Grundlage für die Datenverwendung im Bereich Justiz und Inneres
- Richtlinie – Umsetzung in österreichisches Recht notwendig

Auswirkungen auf Österreich

- DSG wird es weiterhin geben, aber umfassende Novellierung oder Neuerlassung erforderlich
- Regelungsinhaltes des DSG „neu“:
 - Struktur der Aufsichtsbehörde
 - Verfahren vor der Aufsichtsbehörde
 - Neuordnung des datenschutzrechtlichen Meldeverfahrens
 - Schutz juristischer Personen (?)
 - Datenschutz im Bereich Justiz und Inneres und in den sonstigen Bereichen

Definitionen

- § 4 – Art. 4
- personenbezogene Daten – nur noch natürliche Personen!
- Datenanwendungen - Verarbeitungstätigkeiten
- Auftraggeber – Verantwortlicher
- Dienstleister - Auftragverarbeiter

Kapitel VI – Unabhängigkeit der Aufsichtsbehörden

- Eine oder mehrere Aufsichtsbehörde(n) in jedem Mitgliedstaat (Art. 51)
- Mitglieder der Aufsichtsbehörden unterliegen keinen externen Weisungen bei der Erfüllung ihrer Aufgaben und Befugnisse (Art. 52 Abs. 2)
- Aufsichtsbehörde hat Personalhoheit (Art. 52 Abs. 5)
- Sicherstellung der personellen, räumlichen und technischen Ausstattung (Art. 52 Abs. 4)
- Eigenes Budget, das aber auch Teil eines übergeordneten Budgets sein kann (Art. 52 Abs. 6)

Kapitel VI – Unabhängigkeit der Aufsichtsbehörden

- Mitglied/er der Aufsichtsbehörden wird/werden im Rahmen eines transparenten Verfahrens ernannt
 - vom Parlament
 - von der Regierung
 - vom Staatsoberhaupt
 - oder von einer unabhängigen Stelle, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird (Art. 53 Abs. 1)

Kapitel VI – Unabhängigkeit der Aufsichtsbehörden

- Funktionsperiode: zumindest vier Jahre (Art. 54 Abs. 1)
- Mitglied/er der Aufsichtsbehörde muss/müssen entsprechende Qualifikationen aufweisen (Art. 53 Abs. 2)
- Beendigung der Funktion durch Zeitablauf, Rücktritt, Versetzung in den Ruhestand oder Amtsenthebung (Art. 53 Abs. 3 und 4)

Kapitel VI – Unabhängigkeit der Aufsichtsbehörden

- Ausübung der hoheitlichen Befugnisse im eigenen Staatsgebiet (Art. 55 Abs. 1)
- Keine Zuständigkeit für die Überwachung der von Gerichten im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Verarbeitungen (Art. 55 Abs. 3)
- Sofern keine Zuständigkeit der federführenden (ff) Aufsichtsbehörde (One-Stop-Shop) gegeben ist, führt die zuständige Aufsichtsbehörde die (grenzüberschreitenden) Verfahren

Kapitel VI –

Räumliche Zuständigkeit der Aufsichtsbehörde (Art. 55)

- Zuständigkeit für die Ahndung von Rechtsverletzung auf dem eigenen Staatsgebiet, v.a. wenn
 - der Verantwortliche oder Auftragsverarbeiter seinen Sitz im Staatsgebiet hat
 - es sich um eine Behörde oder einen beliebigen Rechtsträger des Mitgliedsstaates handelt
 - eine Datenanwendung von einem Verantwortlichen oder Auftragsverarbeiter mit Sitz in einem Drittstaat betrieben wird und die Datenanwendung auf Betroffene im eigenen Staatsgebiet abzielt
 - ggf. Abstimmung mit ff Aufsichtsbehörde im OSS-Mechanismus notwendig

Kapitel VI –

Aufgaben der Aufsichtsbehörde (Art. 57)

- kann Standardvertragsklauseln im Einklang mit dem Kohärenzverfahren festlegen
- kann Aufzeichnungen von Datenkategorien (= Datenanwendungen) vom Auftraggeber etc. anfordern
- hat Meldungen von Datenschutz-Verletzungen entgegenzunehmen und prüft die Auswirkungen bzw. die getroffenen Gegenmaßnahmen
- hat eine Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, zu erstellen und veröffentlicht diese. Sie hat diese Liste im Kohärenzverfahren abzustimmen

Kapitel VI – Aufgaben der Aufsichtsbehörde (Art. 57)

- kann eine Liste der Verarbeitungsvorgänge erstellen, für die keine Datenschutz-Folgenabschätzung durchzuführen ist
- wird aufgrund Artikel 36 in Anspruch („Vorherige Konsultation“) genommen („zu Rate gezogen“)
- nimmt die Daten der Datenschutzbeauftragten entgegen

Kapitel VI – Aufgaben der Aufsichtsbehörde (Art. 57)

- nimmt zu Entwürfen von Verhaltensregeln Stellung, genehmigt diese und nimmt diese in ein Verzeichnis auf. Wenn sich Verhaltensregeln auf mehrere Mitgliedsstaaten auswirken, legt die Aufsichtsbehörde diese dem EDSA vor
- überwacht die Einhaltung der Verhaltensregeln, kann hierfür eine besonderes geeignete Stelle akkreditieren
- übermittelt einen Entwurf der Akkreditierungskriterien an den EDSA

Kapitel VI – Aufgaben der Aufsichtsbehörde (Art. 57)

- kann die Akkreditierung widerrufen
- kann Zertifizierungen erteilen, verlängern und widerrufen
- kann Zertifizierungsstellen akkreditieren, deren Akkreditierungen verlängern oder widerrufen

Kapitel VI – Aufgaben der Aufsichtsbehörde (Art. 57)

- nimmt von der Zertifizierungsstelle die Gründe einer Zertifizierung bzw. für deren Widerruf entgegen
- veröffentlicht die Anforderungen an eine Zertifizierungsstelle
- Anregung von Datenschutzzertifizierungen und Billigung von Zertifizierungskriterien, Förderung von Datenschutzsiegeln

Kapitel VI – Aufgaben der Aufsichtsbehörde (Art. 57)

- Zurverfügungstellung von Informationen über die Ausübung von Betroffenenrechten auf Antrag von Betroffenen
- Bereitstellung von Online- und Papierbeschwerde- oder Eingabeformularen
- Ablehnungsrecht von Eingaben, wenn diese offenkundig unbegründet oder exzessiv sind, oder Vorschreibung von Kosten

Kapitel VI – Aufgaben der Aufsichtsbehörde (Art. 57)

- Behandlung von Eingaben Betroffener mit Informationspflicht des Betroffenen über den jeweiligen Stand des Verfahrens; Verfahren sind kostenfrei
- Betroffene können sich von spezialisierten Einrichtungen vertreten lassen (Art. 80)

Kapitel VI – Befugnisse der Aufsichtsbehörde (Art. 58)

Art. 58 normiert

- Untersuchungsbefugnisse
- Abhilfebefugnisse
- Genehmigungs- und beratende Befugnisse

**Befugnisse sind gemäß den nationalen
Verfahrensvorschriften und in Übereinstimmung mit
der EU-Grundrechtscharta (GRC) auszuüben**

Kapitel VI –

Befugnisse der Aufsichtsbehörde (Art. 58)

Untersuchungsbefugnisse:

- Anweisung zur Bereitstellung von Informationen
- Durchführung von Untersuchungen im Form von Datenschutzüberprüfungen
- Überprüfung von Zertifizierungen
- Hinweis eines VA od. AV auf einen vermeintlichen Verstoß
- Zugang zu Informationen
- Zutritt zu Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräten

Kapitel VI – Befugnisse der Aufsichtsbehörde (Art. 58)

Abhilfebefugnisse 1:

- Aussprechen von Warnungen (ex ante)
- Aussprechen von Verwarnungen (ex post)
- Anweisung an VA od. AV Anträgen von Betroffenen zu entsprechen
- Anweisung an VA od. AV Verarbeitungsvorgänge in Einklang mit der DSGVO zu bringen
- Auftrag zur Benachrichtigung (Data breach)

Kapitel VI – Befugnisse der Aufsichtsbehörde (Art. 58)

Abhilfebefugnisse 2:

- Verhängung eines Verarbeitungsverbots od. einer Beschränkung der Verarbeitung
- Anordnung der Berichtigung od. Löschung od. der Einschränkung der Verarbeitung
- Widerruf einer Zertifizierung od. Anweisung an Zertifizierungsstelle eine Zertifizierung zu widerrufen bzw. keine zu erteilen
- Verhängung einer Geldbuße zusätzlich zu od. anstelle einer anderen Maßnahme
- Aussetzung des internationalen Datenverkehrs

Kapitel VI –

Befugnisse der Aufsichtsbehörde (Art. 58)

Genehmigungs- und beratende Befugnisse 1:

- Beratung im Rahmen des Konsultationsverfahrens nach Art. 36
- Abgabe von Stellungnahmen an Parlament, die Regierung od. sonstige Stellen
- Genehmigung der Verarbeitung nach Art. 36 Abs. 5
- Erteilung von Zertifizierungen, Billigung von Zertifizierungskriterien
- Akkreditierung von Zertifizierungsstellen

Kapitel VI –

Befugnisse der Aufsichtsbehörde (Art. 58)

Genehmigungs- und beratende Befugnisse 2:

- Stellungnahme zu Verhaltensregeln abgeben und diese ggf. billigen
- Festlegung von Standarddatenschutzklauseln (IDVK, AV)
- Genehmigung von Vertragsklauseln im IDVK
- Genehmigung von Verwaltungsvereinbarungen im IDVK
- Genehmigung von verbindlichen internen Vorschriften im IDVK

Kapitel VI – Befugnisse der Aufsichtsbehörde (Art. 58)

Sonstige Befugnisse:

- ggf. Klagerecht bei Gericht od. Beteiligung am Verfahren
- Anzeigerecht
- Nationales Recht kann weitere Befugnisse festlegen (sofern dadurch die internationale Zusammenarbeit mit anderen Aufsichtsbehörden nicht beeinträchtigt wird)

Kapitel VIII – Rechtsschutz

- Recht auf Beschwerde an ein Gericht gegen verbindliche Entscheidungen der Aufsichtsbehörde (Bescheidbeschwerde) und gegen Säumnis der Aufsichtsbehörde (Säumnisbeschwerde) (Art. 78)
- Betroffene haben Wahlmöglichkeit der Beschwerdeeinbringung: entweder direkt bei Gericht oder bei Aufsichtsbehörde (Parallelverfahren) (Art. 79)

Kapitel VIII – Geldbußen

- Art. 83
- Je nach Verstoß bis zu 20 000 000 Euro od. im Fall eines Unternehmens 4% des gesamten weltweit erzieltes Jahresumsatzes des vorangegangenen Geschäftsjahres
- § 9 VStG – verhältnismäßig?
- uU eigene Bestimmung für die Verantwortlichkeit einer juristischen Person erforderlich (wie im Finanzmarktbereich)

Aufgaben „neu“ f. DSB (Erstbeurteilung)

Stellungnahmen zu
G/V-Entwürfen

Beschwerdewesen,
Verfahrensführung

Entwicklung von
SVK / IDVK

Abnahme v. Verhaltens-
Regel und
Stellungnahmen zu
Entwürfen

Information an
Betroffene über ihre
Rechte

Internationale Amts- u. Rechtshilfe
One – Stop – Shop
Kohärenzverfahren

Kriterien f.
Zertifizierungs-/
Überwachungsstellen
erarbeiten

„Konsultation“

Erstellung einer Liste v.
DAN, für die eine DSFA
durchzuführen
ist / nicht notwendig ist

Stellen akkreditieren

Entgegennahme v.
Meldungen über
Datenschutzverletzungen
Data Breach Notification

Verwaltungsstrafverfahren

SZR

Kapitel VII – Zusammenarbeit und Kohärenz

- ff Aufsichtsbehörde: jene Aufsichtsbehörde, in deren Sprengel der VA/AV seine Hauptniederlassung hat
- ff Aufsichtsbehörde ist von einer anderen Aufsichtsbehörde von Eingaben zu informieren, die einen VA/AV mit Sitz in ihrem Sprengel betrifft

Kapitel VII – Zusammenarbeit und Kohärenz

- ff Aufsichtsbehörde kann Verfahren an sich ziehen und hat alle betroffenen sonstigen Aufsichtsbehörde zu informieren
- ff Aufsichtsbehörde bereitet eine Entscheidung vor und koordiniert sie mit den sonstigen Aufsichtsbehörden
- eine sonstige Aufsichtsbehörde kann dem Entscheidungsentwurf begründet widersprechen; folgt die ff Aufsichtsbehörde dem Widerspruch nicht, kommt das Kohärenzverfahren zur Anwendung

Kapitel VII – Zusammenarbeit und Kohärenz

- ff Aufsichtsbehörde erlässt die Entscheidung und stellt sie dem VA/AV an seiner Hauptniederlassung zu
- wird die Eingabe eines Betroffenen ab- oder zurückgewiesen, bereitet die betroffene Aufsichtsbehörde die Entscheidung vor, stellt sie dem Betroffenen zu und informiert den VA/AV

Kapitel VII – Zusammenarbeit und Kohärenz

- wird die Eingabe tlw. ab-/zurückgewiesen und ihr tlw. stattgegeben, kommt es zur Aufgabenteilung zw. der ff und der betroffenen Aufsichtsbehörde
- VA/AV ist verpflichtet, eine Entscheidung in sämtlichen Niederlassungen im Unionsgebiet umzusetzen

Kapitel VII – Zusammenarbeit und Kohärenz

- Gegenseitige Amtshilfe ohne Notwendigkeit zusätzlicher zwischenstaatlicher Übereinkommen (Art. 61)
- Gemeinsame Maßnahmen (inkl. Mitwirken an Amtshandlungen auf fremden Staatsgebiet, wenn es das Recht des Staates, auf dessen Territorium die Amtshandlung durchgeführt wird, zulässt; Art. 62)
- Möglichkeit der Ergreifung einstweiliger Maßnahmen, wenn Amtshilfeersuchen/Ersuchen um gemeinsame Maßnahme nicht entsprochen wird

Kapitel VII – Zusammenarbeit und Kohärenz

Der Europäische Datenschutzausschuss (EDSA)

- Einrichtung der Union mit eigener Rechtspersönlichkeit
- Löst die Art. 29-Gruppe ab
- Zusammengesetzt aus den Leitern der Aufsichtsbehörden
- EK nimmt an Sitzungen ohne Stimmrecht teil
- EDSB hat eingeschränktes Stimmrecht
- wählt aus seiner Mitte Vorsitz und zwei Stellvertreter (Teilzeit) für fünf Jahre

Inhaltliche Neuerungen

- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutzbeauftragter
- Datenschutz-Folgenabschätzung
- Auskunft, Richtigstellung, Löschung
- Recht auf Datenübertragbarkeit

Verzeichnis von Verarbeitungstätigkeiten

- Art. 30
- Ersetzt DVR-Meldungen
- Totaler Neubeginn
- Inhalte ähnlich
- Behörde darf einsehen
- Inhalt deckt sich weitgehend mit DVR-Meldung

Wer muss das Verzeichnis führen?

- Der Verantwortliche (wie bisher)
- Der Auftragsverarbeiter (neu, bisher nur Pflicht gemäß § 26 Abs. 10 DSGVO 2000!)
- Bei weniger als 250 Mitarbeitern nur
 - Bei erheblichen Risiko für die Rechte und Freiheiten der betroffenen Personen
 - Verarbeitung nicht nur gelegentlich
 - Besondere Daten (Sensible Daten) (Art. 9 Abs. 1), strafbare Handlungen (Art. 10), Achtung bei Biometrie!

Datenschutzbeauftragter I

- Art. 37, 38 und 39
- Muss bestellt werden:
- Bei Behörden
- regelmäßige und systematische Überwachung von betroffenen Personen
- Verarbeitung besonderer Kategorien von Daten oder Daten über strafbare Handlungen
- Recht der Union oder der Mitgliedstaaten (Art. 37 Abs. 4)

Datenschutzbeauftragter II

- Sonst freiwillig!
- Für Verantwortliche und Auftragsverarbeiter
- Eine Gruppe von Unternehmen (Konzerntöchter!) kann einen gemeinsamen Datenschutzbeauftragten bestellen
- Unterrichtung, Beratung, Einhaltung der Vorschriften, Anlaufstelle für die Aufsichtsbehörde

Datenschutz-Folgenabschätzung

- Art. 35-36
- Bei hohem Risiko (neue Technologien, Art, Zweck)
- Abschätzung der Folgen durch den Verantwortlichen (auch Datenschutzbeauftragter)
- Liste der Aufsichtsbehörde
- Wenn hohes Risiko bleibt, Behörde konsultieren!

Auskunft, Richtigstellung, Löschung

- Auskunftsrecht des Betroffenen (Art. 15)
- Recht auf Berichtigung (Art. 16)
- Löschung und „Vergessenwerden“ (Art. 17)

Recht auf Datenübertragbarkeit

- Art. 20
- „Portability“
- Recht auf Kopie eigener Daten in einem Standardform zur Verwendung insb. bei einem anderen Dienst
- Selbst bereitgestellte Daten
- Guidelines on the right to data portability (WP 242)

http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

Weiterführende Informationen

- Website der DSB: www.dsb.gv.at
- Newsletter der DSB: erscheint vierteljährlich und kann unter dsb@dsb.gv.at bestellt werden
- Datenschutzbericht 2015: abrufbar auf der Website der DSB

1 Daten zum Mitnehmen!

Ich kann Daten, die ich einer Organisation oder einem Online-Diensteanbieter zur Verfügung gestellt habe, an andere Diensteanbieter übertragen lassen (soziale Netzwerke, Internet Service Provider, Online-Streaming- Lieferanten etc.).



2 Mehr Transparenz

Ich weiß mehr über das, was mit meinen Daten getan wird und es ist einfacher für mich, meine Rechte zu wahren.



3 Kinderschutz

Online-Dienste müssen vor der Registrierung von Kindern unter 16 Jahren die Einwilligung der Eltern einholen.



4 One-stop-shop

Im Falle von Problemen mit meinen Daten, kann ich mich an meine nationale Datenschutzbehörde wenden, unabhängig von dem Land, in dem eine Organisation meine Daten verarbeitet.



5 Strengere Sanktionen

Wenn eine Verletzung von personenbezogenen Daten stattfindet, kann dies mit bis zu € 20.000.000,- oder 4 % des jährlichen weltweiten Umsatzes bestraft werden.



Illustration: Martin Vothberg

Die Europäische Datenschutz-Grundverordnung

Nach vierjähriger Diskussion auf Ebene der Europäischen Union wurde ein endgültiger Entwurf der Datenschutz-Grundverordnung veröffentlicht. Es wird erwartet, dass Europa damit den Herausforderungen des digitalen Zeitalters besser begegnen kann. Die Verordnung wird die Bürgerrechte stärken und den Bürgern wirkliche Kontrolle über ihre persönlichen Daten geben. Sie wird einen einheitlichen Rahmen für die Unternehmen bieten und die vorherige Meldung vereinfachen. Die Verordnung wird offiziell Anfang 2016 beschlossen werden und im Jahr 2018 in allen EU-Ländern zur Anwendung kommen.

6 Recht auf Vergessenwerden

Ich kann unter bestimmten Umständen Suchmaschinen bitten, Webseiten, die meine Privatsphäre negativ beeinflussen, zu entfernen oder eine Website bitten, Informationen zu löschen.



ARTICLE 29
Data Protection Working Party



Fragen & Antworten