Secur-Data Betriebsberatungsges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at

DSG-Info-Service

Jänner 2017 Ausgabe Nr. 86

Sehr geehrter DSG-Paket-Kunde!
Sehr geehrter Leser!

Knapp vor Weihnachten – am 16. Dezember 2016 – hat die Artikel 29-Gruppe[1] ihre ersten Leitlinien veröffentlicht, die über Details zur Auslegung der ab 25. Mai 2018 in Kraft tretenden Europäischen Datenschutz-Grundverordnung (EU-DSGVO)[2] informieren sollen. Die Artikel 29-Gruppe will mit diesen Leitlinien das Verständnis der DSGVO fördern. Grundsätzlich sind diese Leitlinien ***rechtlich nicht verbindlich****; die EU-Institutionen sind frei, ihren Empfehlungen zu folgen. Sie dienen aber als Orientierungshilfe sowohl für die nationalen Aufsichtsbehörden als auch für Unternehmen.*

Die Artikel 29-Gruppe wird mit Inkrafttreten der DSGVO durch den europäischen Datenschutzausschuss ersetzt, wobei die Zusammensetzung dieses Gremiums nahezu gleich bleibt. So besteht der Ausschuss aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaates, dem Europäischen Datenschutzbeauftragten (EDSB) und einem Vertreter der Europäischen Kommission.

Aktuell behandeln die Leitlinien und die gemeinsam mit diesen veröffentlichten FAQs folgende Themen:

- *Datenübertragbarkeit (Art. 20 DSGVO), WP 242[3]*
- *Datenschutzbeauftragter (Art. 37 DSGVO), WP 243[4]*
- *Zuständigkeit der federführenden Aufsichtsbehörde (Art. 56 DSGVO), WP 244[5]*

[1] http://ec.europa.eu/justice/data-protection/index_en.htm

[2] http://eur-lex.europa.eu/legal-content/DE/ALL/?qid=1483533509146&uri=CELEX%3A32016R0679

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

[4] http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

[5] http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf

1. Leitlinie „Datenübertragbarkeit“ (Art. 20 DSGVO)

Artikel 20 **„Recht auf Datenübertragbarkeit“** lautet wie folgt:

(1) Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

a) die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder

Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und

b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

(2) Bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Absatz 1 hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

(3) Die Ausübung des Rechts nach Absatz 1 des vorliegenden Artikels lässt Artikel 17 unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

(4) Das Recht gemäß Absatz 2 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Der auf Art. 20 bezugnehmende Erwägungsgrund 68 lautet wie folgt:

Um im Fall der Verarbeitung personenbezogener Daten mit automatischen Mitteln eine bessere Kontrolle über die eigenen Daten zu haben, sollte die betroffene Person außerdem berechtigt sein, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten und sie einem anderen Verantwortlichen zu übermitteln. Die Verantwortlichen sollten dazu aufgefordert werden, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen. Dieses Recht sollte dann gelten, wenn die betroffene Person die personenbezogenen Daten mit ihrer Einwilligung zur Verfügung gestellt hat oder die Verarbeitung zur Erfüllung eines Vertrags erforderlich ist. Es sollte nicht gelten, wenn die Verarbeitung auf einer anderen Rechtsgrundlage als ihrer Einwilligung oder eines Vertrags erfolgt. Dieses Recht sollte naturgemäß nicht gegen Verantwortliche ausgeübt werden, die personenbezogenen Daten in Erfüllung ihrer öffentlichen Aufgaben verarbeiten. Es sollte daher nicht gelten, wenn die Verarbeitung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder für die Wahrnehmung einer ihm übertragenen Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung einer ihm übertragenen öffentlichen Gewalt erfolgt, erforderlich ist. Das Recht der betroffenen Person, sie betreffende personenbezogene Daten zu übermitteln oder zu empfangen, sollte für den Verantwortlichen nicht die Pflicht begründen, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten. Ist im Fall eines bestimmten Satzes personenbezogener Daten mehr als eine betroffene Person tangiert, so sollte das Recht auf Empfang der Daten die Grundrechte und Grundfreiheiten anderer betroffener Personen nach dieser Verordnung unberührt lassen. Dieses Recht sollte zudem das Recht der betroffenen Person auf Löschung ihrer personenbezogenen Daten und die Beschränkungen dieses Rechts gemäß dieser Verordnung nicht berühren und insbesondere nicht bedeuten, dass die Daten, die sich auf die betroffene Person beziehen und von ihr zur Erfüllung eines Vertrags zur Verfügung gestellt worden sind, gelöscht werden, soweit und solange diese personenbezogenen Daten für die Erfüllung des Vertrags notwendig sind. Soweit technisch machbar, sollte die betroffene Person das Recht haben, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden.

Die ursprüngliche Intention dieser Regelung war, dass der Betroffene ohne besondere Schwierigkeiten von einem sozialen Medium zu einem anderen wechseln kann. In der endgültigen Fassung der DSGVO wurde aber die Wirkung dieser Bestimmung ausgedehnt. Damit hat der Betroffene, der dem Verantwortlichen Daten zur Verfügung stellt, das Recht,

seine Daten in einem **gängigen** und **maschinenlesbaren Format** zu erhalten bzw. ohne Behinderung an einen anderen Auftraggeber weiterzugeben, sofern folgende Voraussetzungen gegeben sind:

- Die Verarbeitung erfolgte auf Basis einer vorherigen Zustimmung des Betroffenen gem. Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a oder beruht auf einem Vertrag gem. Art. 6 Abs. 1 lit. b und
- die Verarbeitung erfolgte mithilfe automatisierter Verfahren.

Bei Vorliegen der beiden nachfolgenden Ausnahmetatbestände sind die Bestimmungen des Art. 20 nicht anzuwenden, und zwar, wenn

- die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Auftraggeber übertragen wurde (Art. 20 Abs. 3 S 2)
- die Offenlegung personenbezogener Daten die Rechte an geistigem Eigentum in Zusammenhang mit der Verarbeitung dieser personenbezogener Daten verletzen würde (Art. 20 Abs. 4).

Die Leitlinie der Art. 29-Gruppe versucht nun, folgende Bestimmungen klarzulegen, was aber in vielen Fällen nicht gelingt:

- Das Recht auf Datenübertragbarkeit umfasst nur jene Daten, die vom Betroffenen zur Verfügung gestellt worden sind (zB E-Mail-Adresse, Benutzername, Alter usw.) sowie auch jene Daten, die er durch seine Handlungen erzeugt hat (zB Pulsfrequenzdaten von Smart Watches, Verkehrsdaten, Standortdaten, Stromverbrauche, die mit Smart Meter erfasst worden sind, usw.). Das Recht auf Datenübertragung umfasst jedoch nicht jene Daten, die das Ergebnis der weiteren Verarbeitung durch den Verantwortlichen sind (zB Berechnung von Bonitätsmerkmalen, Kaufprofilen usw.)
- Als Werkzeuge für die Übermittlung der Daten an den Betroffenen selbst empfehlen die Leitlinien den direkten Download, für die Übertragung an einen anderen Verantwortlichen die Verwendung eines API (Application Programming Interface). Auch die Möglichkeit einer Datenübertragung auf Wunsch des Betroffenen an einen vertrauenswürdigen Dritten soll möglich sein.
- Die Leitlinie stellt klar, dass der Verantwortliche für die Handhabung der Daten durch den Betroffenen selbst oder einen anderen Verantwortlichen nicht verantwortlich ist. Der andere Verantwortliche ist auch für die Einhaltung der Datenschutzgrundsätze des Art. 5 verantwortlich.
- Das Recht des Betroffenen auf Datenübertragbarkeit schränkt seine anderen Rechte nicht ein.
- Als überzogen ist die Forderung zu werten, dass sowohl der abgebende als auch der empfangende Verantwortliche Werkzeuge zur Verfügung stellen sollen, die es dem Betroffenen ermöglichen, seine Daten von den Daten anderer Betroffener zu trennen.
- Die Betroffenen sind über ihre Rechte auf Datenübertragbarkeit – wie in Art. 13 Abs. 2 lit. b und Art. 14 Abs. 2 lit. c gefordert – zu informieren.
- Weiters empfiehlt die Art. 29-Gruppe, dass der Verantwortliche den Betroffenen auf das Bestehen des Rechts auf Datenübertragbarkeit vor Auflösung eines Kontos (zB Facebook-Account) informiert. Dieser kann dann seine personenbezogenen Daten zwischenspeichern und entweder auf seine eigenen Geräte oder an einen anderen Provider übertragen, bevor der Vertrag ausläuft.
- In Bezug auf die Identitätsprüfung weist die Art. 29-Gruppe darauf hin, dass in der DSGVO keine besonderen Bestimmungen enthalten sind und empfiehlt die Einführung eines Authentifizierungsprozesses.

Ansonsten bleiben die Ausführungen in dieser Hinsicht diffus.

- Der Verantwortliche hat die Datenübertragung an den Betroffenen längstens innerhalb eines Monats durchzuführen; in Ausnahmefällen und bei hoher Komplexität wird eine Frist von drei Monaten zugestanden. Jedenfalls muss der Verantwortliche innerhalb eines Zeitraums von einen Monat reagieren, auch wenn er – aus welchen Gründen immer – der Datenübertragung an den Betroffenen nicht nachkommt. Empfohlen wird die Definition eines Zeitraumes für die Datenübertragung durch den Verantwortlichen und die Bekanntgabe an den Betroffenen
- Die Leitlinie verlangt, dass auch Metadaten gesammelt werden. Als Beispiel wird angeführt, dass es nicht genügt, einem Betroffenen zB PDF-Versionen seines E-Mail-Accounts zu übermitteln, sondern dass dies in einem Format erfolgen muss, das die Wiederverwendbarkeit dieser Daten sicherstellt.
- In Bezug auf die technischen Anforderungen der Datenübertragbarkeit ermutigt die Art. 29-Gruppe die Interessenvertreter der Industrie und der Wirtschaftsverbände zur Zusammenarbeit bei Herstellung von entsprechenden Lösungen.
- Last but not least fordert die Leitlinie, dass sich die Verantwortlichen um die Datensicherheit bei den Betroffenen kümmern sollen.

2. Leitlinie „Datenschutzbeauftragter“ (Art. 37 bis 39 DSGVO)

Art. 37 **„Benennung eines Datenschutzbeauftragten“** lautet wie folgt:

(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,

b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

(2) Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.

(3) Falls es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Stelle handelt, kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.

(4) In anderen als den in Absatz 1 genannten Fällen können der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen; falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen. Der Datenschutzbeauftragte kann für derartige Verbän-

de und andere Vereinigungen, die Verantwortliche oder Auftragsverarbeiter vertreten, handeln.

(5) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.

(6) Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(7) Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

Art. 38 **„Stellung des Datenschutzbeauftragten“** lautet wie folgt:

(1) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(2) Der Verantwortliche und der Auftragsverarbeiter unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 39, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen.

(3) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters.

(4) Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.

(5) Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.

(6) Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

Art. 39 **„Aufgaben des Datenschutzbeauftragten“** lautet wie folgt:

(1) Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

a) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

c) Beratung — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschät-

zung und Überwachung ihrer Durchführung gemäß Artikel 35;

d) Zusammenarbeit mit der Aufsichtsbehörde;

e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

(2) Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Der auf die Art. 37 bis 39 bezugnehmende Erwägungsgrund 97 lautet wie folgt:

In Fällen, in denen die Verarbeitung durch eine Behörde — mit Ausnahmen von Gerichten oder unabhängigen Justizbehörden, die im Rahmen ihrer justiziellen Tätigkeit handeln –, im privaten Sektor durch einen Verantwortlichen erfolgt, dessen Kerntätigkeit in Verarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang erfordern, oder wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht, sollte der Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der internen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person, die über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt, unterstützt werden Im privaten Sektor bezieht sich die Kerntätigkeit eines Verantwortlichen auf seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit. Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die von dem Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich bei ihnen um Beschäftigte des Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.

Die **Leitlinie der Art. 29-Gruppe** versucht, aus den langatmigen und teilweise schwammigen Bestimmungen der Art. 37 bis 39 Klarheit zu einzelnen in der DSGVO verwendeten Begriffen zu gewinnen. Das gelingt jedoch nicht immer.

- Eine verpflichtende Bestellung eines Datenschutzbeauftragten gem. Art. 37 ist in nachstehenden Fällen verpflichtend, und zwar für
  - Behörden oder öffentliche Stellen mit Ausnahme von Gerichten, soweit sie gerichtlich tätig sind (Art. 37 Abs. 1 lit. a)
  - Unternehmen sowie Auftragsverarbeiter, wenn deren **Kerntätigkeit** in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke eine umfangreiche, regelmäßige und systematische Überwachung von Betroffenen erforderlich macht (Art. 37 Abs. 1 lit. b)
  - Unternehmen sowie Auftragsverarbeiter, deren Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem. Art. 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 besteht (Art. 37 Abs. 1 lit. c)
- Die Art. 29-Gruppe empfiehlt die Benennung eines Datenschutzbeauftragten auf freiwilliger Basis, selbst wenn dies nach den Bestimmungen der DSGVO nicht verpflichtend ist. In diesem Fall gelten allerdings ebenfalls die in den Art. 37 bis 39 enthaltenen Bestimmungen.

- Die Leitlinie stellt klar, dass der Datenschutzbeauftragte bei Nicht-Konformität mit den Bestimmungen der DSGVO nicht verantwortlich ist. Nach Meinung der Art. 29-Gruppe stellt die DSGVO klar, dass der Verantwortliche bzw. Auftragsverarbeiter dafür verantwortlich ist, dass die Verarbeitung in Übereinstimmung mit den Bestimmungen der DSGVO erfolgt, und dass dieser das auch nachweisen können muss.
- Die Leitlinie empfiehlt den Entscheidungsprozess, ob nun ein Datenschutzbeauftragter ernannt wird oder nicht, zu dokumentieren.
- Es wird festgestellt, dass die DSGVO die Begriffe „Behörde“ und „öffentliche Stelle“ nicht definiert und daher die jeweils nationale Rechtslage entscheidend ist.
  So definiert § 4 Z 1 IWG in Österreich den Begriff „öffentliche Stelle“ wie folgt:

1. öffentliche Stelle:

a) der Bund,

b) bundesgesetzlich eingerichtete Selbstverwaltungskörperschaften,

c) Einrichtungen auf bundesgesetzlicher Grundlage wie Stiftungen, Privatstiftungen, Fonds und Anstalten sowie sonstige Körperschaften des öffentlichen Rechts, die

- *zu dem besonderen Zweck gegründet wurden, im Allgemeininteresse liegende Aufgaben zu erfüllen, die nicht gewerblicher Art sind und*
- *zumindest teilrechtsfähig sind und*
- *überwiegend vom Bund, von anderen Einrichtungen auf bundesgesetzlicher Grundlage oder von sonstigen öffentlichen Stellen (Art. 2 Z 1 der Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors, ABl. Nr. L 345 vom 31.12.2003 S. 90) finanziert werden oder hinsichtlich ihrer Leitung der Aufsicht durch diese unterliegen oder deren Verwaltungs-, Leitungs- oder Aufsichtsorgan mehrheitlich aus Mitgliedern besteht, die vom Bund, von anderen Einrichtungen auf bundesgesetzlicher Grundlage oder von sonstigen öffentlichen Stellen (Art. 2 Z 1 der Richtlinie 2003/98/EG) ernannt worden sind,*

d) Unternehmungen im Sinne des Art. 126b Abs. 2 B-VG, des Art. 127 Abs. 3 B-VG und des Art. 127a Abs. 3 B-VG, die

- *zu dem besonderen Zweck gegründet wurden, im Allgemeininteresse liegende Aufgaben zu erfüllen, die nicht gewerblicher Art sind und*
- *überwiegend von Bund, Ländern, Gemeinden oder anderen Einrichtungen auf bundes- oder landesgesetzlicher Grundlage finanziert werden oder hinsichtlich ihrer Leitung der Aufsicht durch diese unterliegen oder deren Verwaltungs-, Leitungs- oder Aufsichtsorgan mehrheitlich aus Mitgliedern besteht, die von Bund, Ländern, Gemeinden oder anderen Einrichtungen auf bundes- oder landesgesetzlicher Grundlage ernannt worden sind, wobei das Erfordernis der Gemeindeeinwohnerzahl von 10 000 für Unternehmungen gemäß Art. 127a Abs. 3 B-VG unbeachtlich ist,*

e) Verbände, die sich überwiegend aus zwei oder mehreren öffentlichen Stellen gemäß lit. a bis d zusammensetzen.

- Als Beispiel für den Begriff **„Kerntätigkeit“** führt die Leitlinie ein Spital an, das Gesundheitsdaten verarbeitet, sowie ein privates Sicherheitsunternehmen, das eine Anzahl von privaten Geschäftszentren und öffentliche Plätze per Video überwacht. Bei diesen beiden Beispielen ist jedenfalls die Benennung eines Datenschutzbeauftragten erforderlich.
  Andererseits bedarf es keiner Benennung eines Datenschutzbeauftragten aufgrund von Verarbeitungen aus dem Bereich der Lohn- und Gehaltsverrechnung, da es sich

dabei um eine sogenannte Hilfs- und Nebentätigkeit handelt.

- Unter den Begriff **„umfangreich“** führt die Leitlinie als zu berücksichtigende Faktoren an:
  - Anzahl der Betroffenen
  - Datenmenge und/oder Umfang der Datenarten
  - Dauer oder Konstanz der Verarbeitung
  - Geografische Reichweite der Verarbeitungstätigkeiten

  Als Beispiele für **„umfangreiche Verarbeitung“** werden genannt:
  - Die regelmäßige Verarbeitung von Patientendaten durch ein Spital
  - Die Verarbeitung von Reisedaten von Personen durch ein öffentlichen Transportunternehmen (zB Tracking per Netzkarten)
  - Verarbeitung von Geodaten von Kunden einer internationalen Fastfood-Kette in Echtzeit für statistische Zwecke durch einen Auftragsverarbeiter, der auf die Erbringung dieser Dienstleistung spezialisiert ist
  - Regelmäßige Verarbeitung von Kundendaten durch eine Versicherungsgesellschaft oder eine Bank
  - Die Verarbeitung von personenbezogenen Daten für verhaltensorientierte Werbung („behavioural advertising“) durch eine Suchmaschine
  - Die Verarbeitung von Inhalts-, Verkehrs- und Standortdaten durch einen Telefon- oder Internet Service Provider

  Als Beispiele für **„nicht umfangreiche Verarbeitung“** werden genannt:
  - die Verarbeitung von Patientendaten durch einen Arzt
  - die Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten
- Unter dem Begriff **„umfangreiche, regelmäßige und systematische Überwachung“** von betroffenen Personen führt die Leitlinie unter Bezugnahme auf Erwägungsgrund 24 an, dass unter diesem Begriff unmissverständlich alle Formen von Tracking und Profiling im Internet einschließlich der Profilbildung für verhaltensorientierte Werbung zu verstehen sind. Weiters wird betont, dass der Begriff **„Überwachen“** nicht auf Onlineumgebungen und Onlinetracking beschränkt ist, sondern dass diese nur als Beispiele herangezogen wurden.
  Der Begriff **„regelmäßige Verarbeitung“** wird wie folgt interpretiert:
  - laufend oder in bestimmten Intervallen für eine spezielle Periode
  - wiederkehrend oder mehrmals zu bestimmten Zeitpunkten
  - dauernd oder periodisch stattfindend
- Der Begriff **„systematische Verarbeitung“** wird wie folgt interpretiert:
  - einem System folgend
  - vereinbarungsgemäß, organisiert oder methodisch
  - Teil eines generellen Plans zur Datenermittlung
  - Teil einer Strategie
- Als Beispiele für eine **„regelmäßige und systematische Überwachung“** werden angeführt:
  - Telekommunikationsnetzwerke
  - Telekommunikationsprovider
  - E-Mail-Werbung
  - Profiling und Scoring für Zwecke der Risikoanalyse (zB zur Überprüfung der Kreditwürdigkeit, Festlegung von Versi-

cherungsprämien, Betrugsprävention, Aufdeckung von Geldwäsche)

- Standort-Tracking (zB durch mobile Apps, Kundenbindungsprogramme, verhaltensorientierte Werbung, Wellness-, Fitness- und Gesundheitsdaten durch tragbare Geräte, Videoüberwachung, fest angeschlossene Geräte wie Smart Meter, Smart Cars und Heimautomatisierung)

- Die Leitlinie weist darauf hin, dass Art. 37 sowohl für den „**Verantwortlichen**" als auch für den „**Auftragsverarbeiter**" gilt. In manchen Fällen muss aber **nur** der Verantwortliche, in anderen Fällen **nur** der Auftragsverarbeiter und in wieder anderen Fällen müssen **beide** einen Datenschutzbeauftragten benennen. Als Beispiele werden angeführt:
  - Ein kleines Familienunternehmen, das Haushaltsgeräte in einer einzigen Stadt verkauft und dazu die Dienstleistungen eines Auftragsverarbeiters in Anspruch nimmt, der Webanalysen und Unterstützung bei targeted advertising („zielgerichtete Werbung") und Marketing anbietet, benötigt keinen Datenschutzbeauftragten, da seine Aktivitäten – geringe Kundenanzahl und relativ eingeschränkte Aktivitäten –- als „nicht umfangreich" einzustufen sind. Der Auftragsverarbeiter dagegen, der seine Dienstleistungen vielen Kunden anbietet, führt „umfangreiche Verarbeitungen" durch und benötigt daher einen Datenschutzbeauftragten.
  - Ein mittlerer Ziegelproduzent, der seine Gesundheitsvorsorge für die Mitarbeiter an einen externen Gesundheitsdiensteanbieter auslagert, benötigt keinen Datenschutzbeauftragten. Der Gesundheitsdiensteanbieter dagegen, der eine große Anzahl ähnlicher Kunden betreut, benötigt **einen** Datenschutzbeauftragten.

- Gem. Art. 37 Abs. 2 kann eine Unternehmensgruppe einen gemeinsamen Datenschutzbeauftragten ernennen, sofern dieser „von jeder Niederlassung aus leicht erreicht werden kann". Diese „leichte Erreichbarkeit" ist im Zusammenhang mit den Aufgaben des Datenschutzbeauftragten als Kontaktperson für die Betroffenen, für die Aufsichtsbehörden, aber auch für die interne Organisation zu sehen. Er muss in der Lage sein, effizient mit den Betroffenen und den Aufsichtsbehörden kommunizieren zu können.
  Diese Voraussetzungen betreffen auch einen Datenschutzbeauftragten, der gem. Art 37 Abs.3 für mehrere Behörden oder öffentliche Stellen tätig wird: Der Verantwortliche muss sich vergewissern, dass der Datenschutzbeauftragte seine Aufgaben effizient wahrnehmen kann, ungeachtet dessen, dass er für mehrere Behörden und öffentliche Stellen tätig ist.

- Der Datenschutzbeauftragte unterliegt gem. Art. 38 Abs. 5 der Geheimhaltungspflicht der EU oder des jeweiligen Mitgliedsstaates.

- Hinsichtlich der beruflichen Qualifikation und Fähigkeiten des Datenschutzbeauftragten bietet die Leitlinie außer allgemeinen Floskeln keine weiterführenden Erkenntnisse.

- Die Leitlinie betont, dass die Position des Datenschutzbeauftragten auch auf Basis eines Dienstleistungsvertrages (Werkvertrag) mit einer natürlichen Person oder einem Unternehmen wahrgenommen werden kann. Wird die Funktion durch ein externes Unternehmen wahrgenommen, so muss sichergestellt sein, dass jeder Mitarbeiter dieses Unternehmens alle Anforderungen des Abschnitt 4 DSGVO abdecken kann (Abschnitt 4 umfasst die Art. 37 bis einschließlich 39). Vor allem ist es notwendig, dass keiner dieser Mitarbeiter in einem Interessenskonflikt mit dem Verantwortlichen steht. Es ist weiters wichtig, dass für die extern bestellten Datenschutzbeauf-

tragten auch die Schutzmaßnahmen der DSGVO – keine ungerechte Kündigung des Dienstleistungsvertrages, keine ungerechte Kündigung eines einzelnen Mitarbeiters dieses Unternehmens – Geltung haben.

- Gem. Art. 37 Abs. 7 müssen die Kontaktdaten des Datenschutzbeauftragten veröffentlicht und der Aufsichtsbehörde mitgeteilt werden.
- Die Leitlinie empfiehlt dem Verantwortlichen, dass er den Datenschutzbeauftragten schon frühzeitig in alle Fragen der Datenverarbeitung einbezieht, vor allem bei der gem. Art 35 vorgeschriebenen Datenschutz-Folgenabschätzung. Darüber hinaus ist es wichtig, dass der Datenschutzbeauftragte als „Diskussionspartner" innerhalb der Organisation angesehen wird. Bei Nicht-Übereinstimmung mit den Empfehlungen des Datenschutzbeauftragten sollte der Verantwortliche die Gründe dokumentieren.
- In Bezug auf die gem. Art. 38 Abs. 2 geforderte Zurverfügungstellung der erforderlichen Ressourcen durch den Verantwortlichen oder Auftragsverarbeiter führt die Leitlinie folgendes an:
  - Aktive Unterstützung des Datenschutzbeauftragten durch die Führungskräfte (z.B. Vorstandsebene)
  - Ausreichend Zeit zur Wahrnehmung der Pflichten des Datenschutzbeauftragten, besonders in Fällen, wo der Datenschutzbeauftragte auch andere Aufgaben im Unternehmen wahrnimmt
  - Ausreichende Unterstützung in Bezug auf Finanzmittel, Infrastruktur (Büro und Ausstattung) sowie bei Notwendigkeit auch Mitarbeiter
  - Bekanntmachung der Benennung eines Datenschutzbeauftragten an alle Mitarbeiter
  - Bereitstellung der nötigen Zugriffsmöglichkeiten auf andere interne Dienste wie HR, Recht, IT, Sicherheit usw.
  - Regelmäßige Schulungen, um sein Wissen aktuell zu halten
  - Abhängig von der Größe und der Struktur der Organisation kann es auch notwendig sein, ein Datenschutz-Team einzurichten.
- Gem. Art. 38 Abs. 3 ist sicherzustellen, dass der Datenschutzbeauftragte weisungsfrei arbeiten kann und auf Grund seiner Tätigkeit weder gekündigt werden kann noch sonstige Nachteile erleidet. Das bedeutet aber laut Leitlinie nicht, dass er über seine Aufgaben gem. Art. 39 hinaus über Entscheidungskompetenz verfügt.
- Laut DSGVO sind Sanktionen gegen den Datenschutzbeauftragten aufgrund der Wahrnehmung seiner Aufgaben verboten. Diese Bestimmung schießt jedoch nicht arbeitsrechtliche oder strafrechtliche Folgen bei anderen Vergehen aus.
- Zur in Art. 38 Abs. 6 enthaltenen Forderung der Sicherstellung, dass der Datenschutzbeauftragte bei der Wahrnehmung anderer Aufgaben keinem Interessenskonflikt ausgesetzt sein sollte, enthält die Leitlinie nur Gemeinplätze.
- In Bezug auf die in Art. 39 Abs. 1 lit b enthaltene Bestimmung, dass der Datenschutzbeauftragte die Einhaltung der DSGVO überwachen soll (Monitoring), stellt die Art. 29-Gruppe klar, dass der Datenschutzbeauftragte **nicht** für die Nicht-Konformität mit der DSGVO verantwortlich ist, sondern **allein** der Verantwortliche oder der Auftragsverarbeiter.
- Die Leitlinie weist darauf hin, dass die Durchführung einer Datenschutz-Folgenabschätzung Aufgabe des Verarbeiters und nicht des Datenschutzbeauftragten ist. Sie führt aber an, dass der Datenschutzbeauftragte dabei eine wichtige und wertvolle Rolle spielen kann, indem er den

Verantwortlichen bei der Durchführung dieser Aufgabe unterstützt, und zwar bei der Beantwortung folgender Fragen:

- Muss eine Datenschutz-Folgenabschätzung durchgeführt werden oder nicht?
- Welche Methode soll verfolgt werden?
- Soll die Datenschutz-Folgenabschätzung intern oder extern durchgeführt werden?
- Welche Sicherheitsmaßnahmen (einschließlich technischer und organisatorischer Maßnahmen) sollen angewendet werden, um die Risken in Bezug auf die Rechte und Freiheiten natürlicher Personen zu entschärfen?
- Wurde die Datenschutz-Folgenabschätzung ordnungsgemäß durchgeführt und stehen die Schlussfolgerungen in Einklang mit der DSGVO?

- Die in Art. 39 Abs. 2 enthaltene Bestimmung, wonach der Datenschutzbeauftragte bei der „Erfüllung seiner Aufgaben den mit der Verarbeitung verbundenen Risken gebührend Rechnung trägt“, bedeutet laut Leitlinie, dass der Datenschutzbeauftragte auch bei seiner Tätigkeit einen risikobasierten Ansatz verfolgt. Das heißt, dass er sich schwerpunktmäßig auf jene Bereiche konzentriert, bei denen hohes Risiko gegeben ist.

Die Leitlinie stellt außerdem klar, dass das gem Art. 30 Abs. 1 und 2 zu führende „Verfahrensverzeichnis“ vom Verantwortlichen oder Auftragsverarbeiter zu führen ist, aber **nicht** vom Datenschutzbeauftragten. Es spricht andererseits aber nichts dagegen, dass der Verantwortliche oder Auftragsverarbeiter den Datenschutzbeauftragten mit der Führung der Verfahrensverzeichnisse beauftragt.

3. Leitlinie „Zuständigkeit der federführenden Aufsichtsbehörde“ (Art. 56 DSGVO)

Art. 56 **„Zuständigkeit der federführenden Aufsichtsbehörde“** lautet wie folgt:

(1) Unbeschadet des Artikels 55 ist die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters gemäß dem Verfahren nach Artikel 60 die zuständige federführende Aufsichtsbehörde für die von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführte grenzüberschreitende Verarbeitung.

(2) Abweichend von Absatz 1 ist jede Aufsichtsbehörde dafür zuständig, sich mit einer bei ihr eingereichten Beschwerde oder einem etwaigen Verstoß gegen diese Verordnung zu befassen, wenn der Gegenstand nur mit einer Niederlassung in ihrem Mitgliedstaat zusammenhängt oder betroffene Personen nur ihres Mitgliedstaats erheblich beeinträchtigt.

(3) In den in Absatz 2 des vorliegenden Artikels genannten Fällen unterrichtet die Aufsichtsbehörde unverzüglich die federführende Aufsichtsbehörde über diese Angelegenheit. Innerhalb einer Frist von drei Wochen nach der Unterrichtung entscheidet die federführende Aufsichtsbehörde, ob sie sich mit dem Fall gemäß dem Verfahren nach Artikel 60 befasst oder nicht, wobei sie berücksichtigt, ob der Verantwortliche oder der Auftragsverarbeiter in dem Mitgliedstaat, dessen Aufsichtsbehörde sie unterrichtet hat, eine Niederlassung hat oder nicht.

(4) Entscheidet die federführende Aufsichtsbehörde, sich mit dem Fall zu befassen, so findet das Verfahren nach Artikel 60 Anwendung. Die Aufsichtsbehörde, die die federführende Aufsichtsbehörde unterrichtet hat, kann dieser einen Beschlussentwurf vorlegen. Die federführende Aufsichtsbehörde trägt diesem Entwurf bei der Ausarbeitung des Beschlussent-

wurfs nach Artikel 60 Absatz 3 weitestgehend Rechnung.

(5) Entscheidet die federführende Aufsichtsbehörde, sich mit dem Fall nicht selbst zu befassen, so befasst die Aufsichtsbehörde, die die federführende Aufsichtsbehörde unterrichtet hat, sich mit dem Fall gemäß den Artikeln 61 und 62.

(6) Die federführende Aufsichtsbehörde ist der einzige Ansprechpartner der Verantwortlichen oder der Auftragsverarbeiter für Fragen der von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführten grenzüberschreitenden Verarbeitung.

Die auf Art. 56 Bezug nehmenden Erwägungsgründe 124, 125, 126, 127 und 128 lauten wie folgt:

(124) Findet die Verarbeitung personenbezogener Daten im Zusammenhang mit der Tätigkeit einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union statt und hat der Verantwortliche oder der Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat oder hat die Verarbeitungstätigkeit im Zusammenhang mit der Tätigkeit einer einzigen Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat bzw. wird sie voraussichtlich solche Auswirkungen haben, so sollte die Aufsichtsbehörde für die Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters oder für die einzige Niederlassung des Verantwortlichen oder Auftragsverarbeiters als federführende Behörde fungieren. Sie sollte mit den anderen Behörden zusammenarbeiten, die betroffen sind, weil der Verantwortliche oder Auftragsverarbeiter eine Niederlassung im Hoheitsgebiet ihres Mitgliedstaats hat, weil die Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz in ihrem Hoheitsgebiet hat oder weil bei ihnen eine Beschwerde eingelegt wurde. Auch wenn eine betroffene Person ohne Wohnsitz in dem betreffenden Mitgliedstaat eine Beschwerde eingelegt hat, sollte die Aufsichtsbehörde, bei der Beschwerde eingelegt wurde, auch eine betroffene Aufsichtsbehörde sein. Der Ausschuss sollte — im Rahmen seiner Aufgaben in Bezug auf die Herausgabe von Leitlinien zu allen Fragen im Zusammenhang mit der Anwendung dieser Verordnung — insbesondere Leitlinien zu den Kriterien ausgeben können, die bei der Feststellung zu berücksichtigen sind, ob die fragliche Verarbeitung erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat und was einen maßgeblichen und begründeten Einspruch darstellt.

(125) Die federführende Behörde sollte berechtigt sein, verbindliche Beschlüsse über Maßnahmen zu erlassen, mit denen die ihr gemäß dieser Verordnung übertragenen Befugnisse ausgeübt werden. In ihrer Eigenschaft als federführende Behörde sollte diese Aufsichtsbehörde für die enge Einbindung und Koordinierung der betroffenen Aufsichtsbehörden im Entscheidungsprozess sorgen. Wird beschlossen, die Beschwerde der betroffenen Person vollständig oder teilweise abzuweisen, so sollte dieser Beschluss von der Aufsichtsbehörde angenommen werden, bei der die Beschwerde eingelegt wurde.

(126) Der Beschluss sollte von der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden gemeinsam vereinbart werden und an die Hauptniederlassung oder die einzige Niederlassung des Verantwortlichen oder Auftragsverarbeiters gerichtet sein und für den Verantwortlichen und den Auftragsverarbeiter verbindlich sein. Der Verantwortliche oder Auftragsverarbeiter sollte die erforderlichen Maßnahmen treffen, um die Einhaltung dieser Verordnung und die Umsetzung des Beschlusses zu gewährleisten, der der Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters im Hinblick auf die Verarbeitungstätigkeiten in der Union von der federführenden Aufsichtsbehörde mitgeteilt wurde.

(127) Jede Aufsichtsbehörde, die nicht als federführende Aufsichtsbehörde fungiert, sollte in örtlichen Fällen zuständig sein, wenn der Verantwortliche oder Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat hat, der Gegenstand der spezifischen Verarbeitung aber nur die Verarbeitungstätigkeiten in einem einzigen Mitgliedstaat und nur betroffene Personen in diesem einen Mitgliedstaat betrifft, beispielsweise wenn es um die Verarbeitung von personenbezogenen Daten von Arbeitnehmern im spezifischen Beschäftigungskontext eines Mitgliedstaats geht. In solchen Fällen sollte die Aufsichtsbehörde unverzüglich die federführende Aufsichtsbehörde über diese Angelegenheit unterrichten. Nach ihrer Unterrichtung sollte die federführende Aufsichtsbehörde entscheiden, ob sie den Fall nach den Bestimmungen zur Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden gemäß der Vorschrift zur Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden (im Folgenden „Verfahren der Zusammenarbeit und Kohärenz") regelt oder ob die Aufsichtsbehörde, die sie unterrichtet hat, den Fall auf örtlicher Ebene regeln sollte. Dabei sollte die federführende Aufsichtsbehörde berücksichtigen, ob der Verantwortliche oder der Auftragsverarbeiter in dem Mitgliedstaat, dessen Aufsichtsbehörde sie unterrichtet hat, eine Niederlassung hat, damit Beschlüsse gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter wirksam durchgesetzt werden. Entscheidet die federführende Aufsichtsbehörde, den Fall selbst zu regeln, sollte die Aufsichtsbehörde, die sie unterrichtet hat, die Möglichkeit haben, einen Beschlussentwurf vorzulegen, dem die federführende Aufsichtsbehörde bei der Ausarbeitung ihres Beschlussentwurfs im Rahmen dieses Verfahrens der Zusammenarbeit und Kohärenz weitestgehend Rechnung tragen sollte.

(128) Die Vorschriften über die federführende Behörde und das Verfahren der Zusammenarbeit und Kohärenz sollten keine Anwendung finden, wenn die Verarbeitung durch Behörden oder private Stellen im öffentlichen Interesse erfolgt. In diesen Fällen sollte die Aufsichtsbehörde des Mitgliedstaats, in dem die Behörde oder private Einrichtung ihren Sitz hat, die einzige Aufsichtsbehörde sein, die dafür zuständig ist, die Befugnisse auszuüben, die ihr mit dieser Verordnung übertragen wurden.

Auf insgesamt 11 Seiten (!) versucht die **Leitlinie** der **Art. 29-Gruppe** Klarheit und Rechtssicherheit in Bezug auf die Definition der federführenden Aufsichtsbehörde zu schaffen. Das gelingt ihr aber auch in dieser umfangreichen Darstellung keineswegs, wie ja überhaupt das über eineinhalb Jahre diskutierte „One-Stop Shop-Prinzip", das die zentrale Zuständigkeit einer einzelnen Aufsichtsbehörde gewährleisten sollte, gründlich misslungen ist.

- Die Leitlinie führt aus, dass die Bestimmung der federführenden Aufsichtsbehörde nur dann notwendig ist, wenn der Verantwortliche eine **grenzüberschreitende Verarbeitung** durchführt. Als grenzüberschreitend gilt eine Verarbeitung dann, wenn sie in mehr als einem EU-Mitgliedstaat durchgeführt wird oder die Verarbeitung erhebliche Auswirkungen auf Betroffene in mehr als einem Mitgliedsstaat hat.
- Über den Begriff **„erhebliche Auswirkungen"** erfolgt eine langatmige semantische Auseinandersetzung unter Zuhilfenahme des Oxford English Dictionary! Schlussendlich werden folgende Faktoren zur Interpretation dieser Wortfolge genannt:
- Wenn die Verarbeitung
  - Schaden, Verlust oder Gefahr für den Betroffenen verursacht oder wahrscheinlich verursacht,
  - tatsächliche Auswirkungen in Bezug auf die Einschränkung von Rechten oder dem Vorenthalten von Möglichkeiten hat,

- die Gesundheit, das Wohlbefinden oder die Psyche des Betroffenen beeinträchtigt oder wahrscheinlich beeinträchtigt,
- die finanzielle oder wirtschaftliche Lage des Betroffenen beeinträchtigt oder wahrscheinlich beeinträchtigt,
- natürliche Personen diskriminiert oder ungerecht behandelt,
- Analysen von „sensiblen Daten“ oder anderen Daten vornimmt, die in die Privatsphäre eingreifen, insbesondere in Bezug auf Daten von Kindern,
- erhebliche Verhaltensveränderungen von natürlichen Personen hervorruft oder wahrscheinlich hervorruft,
- Peinlichkeiten oder negative Folgen einschließlich Rufschädigung verursacht,
- umfangreiche personenbezogene Daten umfasst.

- Durch diese Aufzählung wird keine Unterstützung bei der zu klärenden Frage erreicht. Die angeführten Faktoren sind zu unbestimmt.
- Die Art. 29-Gruppe versucht anschließend, den in Art. 56 verwendeten Begriff **„Hauptniederlassung“** („Main Establishment“) zu erläutern. Nach diesen Ausführungen ist es notwendig, dass der Verantwortliche festlegt, in welchem Mitgliedsstaat er seine **„Zentrale“** („Hauptniederlassung“) eingerichtet hat. Diese ist jene Unternehmenseinheit innerhalb der EU, die die Entscheidungen über Zwecke und Mittel für die Verarbeitung personenbezogener Daten trifft. Es wird darauf hingewiesen, dass es auch **„mehrere Hauptniederlassungen“** geben kann [Anmerkung: Da es **„die eine“** grenzüberschreitende Verarbeitung in einer Unternehmensgruppe nicht geben wird, wird auch die durch das One-Stop-Shop-Prinzip erwartete administrative Erleichterung und vor allem eine homogene Spruchpraxis nicht erreicht werden].
- Die Leitlinie nennt folgende Faktoren, die zur Bestimmung der „Hauptniederlassung“ heranzuziehen sind:
  - Wo werden die Entscheidungen über den Zweck und die Mittel der Verarbeitung schlussendlich getroffen?
  - Wo werden Entscheidungen über Geschäftsaktivitäten, die eine Datenverarbeitung mit sich bringen, getroffen?
  - Wo liegt die Macht, Entscheidungen effektiv umzusetzen?
  - Wo sitzt der Direktor (bzw. die Direktoren) mit der gesamten Managementverantwortung für die grenzüberschreitende Verarbeitung?
  - Wo ist das Unternehmen des Verantwortlichen oder Auftragsverarbeiters registriert, sofern das in einem einzigen Mitgliedsstaat erfolgt ist?

  Die Art. 29-Gruppe führt aus, dass die DSGVO keine Auswahl des **„günstigsten Gerichtsstandes“** erlaubt. Das bedeutet, dass die Aufsichtsbehörde oder letztendlich der Europäische Datenschutzausschuss („European Data Protection Board“ oder kurz EDPB) im Falle, dass die tatsächliche Entscheidungsgewalt nicht in der vom Unternehmen angegebenen Hauptniederlassung liegt, nach objektiven Kriterien und Lokalaugenschein festlegen kann, dass die Hauptniederlassung in einem anderen Mitgliedstaat liegt.

In einem eigenen Anhang I werden Kriterien zusammengefasst, mit deren Hilfe die „federführende Aufsichtsbehörde“ identifiziert werden kann:

I. Führt der Verantwortliche oder Auftragsverarbeiter eine grenzüberschreitende Verarbeitung durch?

a. Ja, und das Unternehmen ist in einem einzigen Mitgliedsstaat ansässig und verarbeitet personenbezogene Daten nur an diesem Standort, die Verarbeitung beein-

flusst aber wahrscheinlich Betroffene in mehr als einem Mitgliedsstaat. In diesem Fall ist die federführende Aufsichtsbehörde jene des Mitgliedsstaates dieser Niederlassung.

b. Ja, weil der Verantwortliche und/oder Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedsstaat hat und personenbezogene Daten in Zusammenhang mit Aktivitäten zumindest einiger dieser Niederlassungen verarbeitet. In diesem Fall ist bei Punkt II fortzufahren.

II. Identifizierung der federführenden Aufsichtsbehörde

In Zusammenhang mit I b: Betrifft der Fall einen Verantwortlichen oder Auftragsverarbeiter?

a. Falls nur ein Verantwortlicher betroffen ist, identifiziert der Verantwortliche den Ort seiner Hauptniederlassung in der EU.

i. Die Aufsichtsbehörde dieses Mitgliedsstaates ist federführend für die zu prüfende Datenverarbeitung.

ii. Es sei denn, Entscheidungen über die Zwecke und Mittel der Verarbeitung werden in einer anderen Niederlassung in der EU getroffen. Die federführende Aufsichtsbehörde wird dann diesem Land zugemessen.

b. Wenn der Fall sowohl einen Verantwortlichen und einen Auftragsverarbeiter umfasst:

i. Zu prüfen ist, ob der Verantwortliche in der EU niedergelassen ist und sich dem One-Stop-Shop-System unterworfen hat.

ii. Der Ort der federführenden Aufsichtsbehörde des Verantwortlichen ist zu identifizieren. Diese dient dann als federführende Aufsichtsbehörde sowohl für den Verantwortlichen als auch für den Auftragsverarbeiter.

iii. Die für den Auftragsverarbeiter zuständige Aufsichtsbehörde ist als betroffene Behörde anzusehen.

c. Wenn der Fall nur einen Auftragsverarbeiter umfasst:

i. Der Ort der Hauptniederlassung in der EU ist zu identifizieren.

ii. Falls es keine Hauptniederlassung in der EU gibt, sind die Niederlassungen in der EU zu identifizieren, an denen Datenverarbeitungen durchgeführt werden. Anschließend ist zu bestimmen, wo die hauptsächlichen Verarbeitungsaktivitäten stattfinden.

III. Identifizierung der betroffenen Aufsichtsbehörden

Welche anderen Aufsichtsbehörden sind „betroffene Behörden“?

Eine Aufsichtsbehörde kann „betroffen“ sein, wenn der Verantwortliche/-Auftragsverarbeiter in ihrem Land eine Niederlassung hat ODER wenn Betroffene in ihrem Land wesentlich Betroffene oder wahrscheinlich Betroffene sind ODER bei Eingehen einer Beschwerde.

Im Interesse der Wirtschaft – vor allem der digitalen Wirtschaft – bleibt zu hoffen, dass die Europäische Kommission und jene Stellen, die in den Mitgliedstaaten für die Umsetzung der DSGVO verantwortlich sind, mit den Interpretationen der Art. 29-Gruppe **sorgfältig** umgehen werden.

••••

Pollirer/Weiss/Knyrim/Haidinger

DSGVO

Datenschutz-Grundverordnung

Mit Mai 2018 gilt die neue Europäische Datenschutz-Grundverordnung, kurz DSGVO, die in Österreich direkt anwendbar ist. Sie zählt nicht weniger als **99 Artikel** und **173 Erwägungsgründe** – eine Herausforderung für alle, die sich einen ersten Überblick verschaffen, die Rahmenbedingungen kennenlernen und mit den Vorbereitungen starten wollen.

Dieses Starterpaket versorgt Sie mit den **wesentlichen Erstinformationen:**

- Authentischer Text der neuen DSGVO, **übersichtlich** und lesefreundlich
- Materialien zum Entstehungsprozess: **Erwägungsgründe** der passenden Textpassage **zugeordnet**, als **erste Auslegungshilfe**
- Ein **Stichwortverzeichnis** für den alternativen Zugang
- Ein Verzeichnis der **Öffnungsklauseln** – wo besteht noch Handlungsbedarf der nationalen Gesetzgeber?

ISBN: 978-3-214-01167-3
Reihe: Manz Sonderausgaben
Verlag: MANZ Verlag Wien
Format: Flexibler Einband
XII, 214 Seiten, 2017
Preis: EUR 32,00

Die Möglichkeit zur Direktbestellung finden Sie unter www.manz.at