2.2 Entwurf einer EU-E-Privacy-Verordnung

Am 10.01.2017 hat die Europäische Kommission einen Entwurf für eine „Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG" (Verordnung über Privatsphäre und elektronische Kommunikation) vorgelegt.
Da es sich – im Gegensatz zur bisherigen Richtlinie – um eine EU-Verordnung handeln soll, würde die sogenannte E-Privacy-Verordnung nach dem Inkrafttreten unmittelbar geltendes Recht in allen Mitgliedstaaten.

1. Ziele der Verordnung

Die Verordnung soll das Vertrauen in digitale Dienste und deren Sicherheit erhöhen und in Übereinstimmung mit der Datenschutz-Grundverordnung (DSGVO) stehen.(1)
Sie soll den Schutz von Grundrechten und Grundfreiheiten, insbesondere die Achtung des Privatlebens, die Wahrung der Vertraulichkeit der Kommunikation und den Schutz personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr von elektronischen Kommunikationsdaten, -geräten und -diensten in der Union gewährleisten. Außerdem soll sie hinsichtlich der Kommunikation die Umsetzung des in Artikel 7 der Charta der Grundrechte der Europäischen Union („Charta") verankerten Grundrechts auf Achtung des Privatlebens im Sekundärrecht der Union bewirken.

2. Gründe

Zwar behalten die Ziele und Grundsätze der gegenwärtig gültigen e-Datenschutz-Richtlinie weiterhin Gültigkeit, allerdings haben sich seither wichtige technische und wirtschaftliche Entwicklungen auf dem Markt vollzogen. Anstatt herkömmliche Kommunikationsdienste zu nutzen, verlassen sich Verbraucher und Unternehmen zunehmend auf neue Internetdienste, die eine interpersonelle Kommunikation ermöglichen, z. B. VoIP-Telefonie, Sofortnachrichtenübermittlung (Instant-Messaging) und webgestützte E-Mail-Dienste. Solche Over-the-Top-Kommunikationsdienste („OTT-Dienste") werden aber im Allgemeinen vom gegenwärtigen Rechtsrahmen der Union für die elektronische Kommunikation, einschließlich der e-Datenschutz-Richtlinie, nicht erfasst. Folglich hat die Richtlinie mit der technischen Entwicklung nicht Schritt gehalten, was nach Ansicht der EU-Kommission zu

derungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen (Art. 25 Abs. 1 DSGVO).
Auch wenn im Gesetzestext nur die Datenschutzgrundsätze als denkbare Maßnahmen erwähnt werden, kommen natürlich auch andere Maßnahmen in Betracht. Dies wird auch im Erwägungsgrund 78 zur Datenschutz-Grundverordnung deutlich: „Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern."
Weitergehende Aussagen zu den geeigneten technischen und organisatorischen Maßnahmen sind der Datenschutz-Grundverordnung nicht zu entnehmen.
Im Übrigen überschneidet sich der Art. 25 Abs. 1 zum Großteil mit Art. 32 Abs. 1 DSGVO, wird doch in beiden Gesetzesregelungen die Ergreifung technisch-organisatorischer Maßnahmen zur Gewährleistung der Einhaltung der Datenschutz-Grundverordnung verlangt und die Auflistung der Abwägungskriterien ist nahezu identisch.

HINWEIS:

Die einzelnen Auswahlkriterien (Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und die Zwecke der Verarbeitung, Eintrittswahrscheinlichkeit und Schwere des Risikos, geeignete technische und organisatorische Maßnahmen) werden im Kapitel 6.2 Datensicherheitsmaßnahmen besprochen.

a) Umsetzung der Datenschutzgrundsätze

Auch wenn im Art. 25 Abs. 1 DSGVO lediglich die Datenminimierung erwähnt wird, müssen natürlich alle Datenschutzgrundsätze des Art. 5 DSGVO beachtet werden. Diese sind:

- Grundsatz der Rechtmäßigkeit von Treu und Glauben und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit der Daten
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

(3) *Bei genehmigter Verlagerung der Datenverarbeitung in ein Drittland muss das angemessene Schutzniveau*

- □ *festgelegt sein durch einen Angemessenheitsbeschluss der Europäischen Kommission (Art. 45 Abs. 3 DSGVO)*
- □ *hergestellt werden durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 Buchst. b i. V. m. Art. 47 DSGVO)*
- □ *hergestellt werden durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 Buchst. e i. V. m. Art. 40 DSGVO)*
- □ *hergestellt werden durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 Buchst. f i. V. m. Art. 42 DSGVO)*
- □ *hergestellt werden durch sonstige Maßnahmen (Art. 46 Abs. 2 Buchst. a, Abs. 3 Buchst. a und b DSGVO)*

e) Kreis der Betroffenen

Der Kreis der durch diese Auftragsverarbeitung Betroffenen umfasst:

- _ .....
- _ .....
- _ .....
- _ .....
- _ .....

(detaillierte Aufstellung der Betroffenen, z. B. eigene Mitarbeiter, Kunden, Interessenten, Lieferanten)

§ 2 Vertragsdauer

(1) Der Vertrag
beginnt am .....
und
endet

- □ *am* .....
- □ *mit Auftragserledigung.*
- □ *wird auf unbestimmte Zeit geschlossen.*

(2) Der Vertrag ist mit einer Frist von . . . . . Monaten zum Quartalsende kündbar.

(3) Der Auftraggeber ist zu einer außerordentlichen Kündigung des Vertrags berechtigt, wenn der Auftragnehmer trotz schriftlicher Aufforderung die vereinbarten Leistungen nach § 1 nicht ordnungsgemäß erbringt oder seine Pflichten nach § 3 verletzt.

puter viel Zeit. Außerdem sind asymmetrische Verschlüsselungsverfahren bei der Datenübertragung sehr langsam und eignen sich daher nur für sehr kleine Datenmengen.(2)
Ein weiterer Nachteil besteht in der mangelnden Authentizität. Wer etwas mit dem Public Key eines Empfängers verschlüsseln möchte, muss sichergehen können, dass dieser auch wirklich demjenigen gehört. Im Internet ist es leicht sich für jemanden anderen auszugeben und es könnte jemand fälschlicherweise behaupten, er wäre der berechtigte Empfänger. Für die falsche Identität ließen sich problemlos Schlüsselpaare generieren und Public Keys in Umlauf bringen. Der Fälscher könnte dann vertrauliche Botschaften lesen, weil die Absender seinen Schlüssel benutzt haben, statt den des eigentlich gewollten Empfängers. Würde er die Botschaft danach, vielleicht auch noch manipuliert, an den richtigen Empfänger weiterleiten, bliebe das ganze wahrscheinlich auch noch unbemerkt.

Empfohlene Schlüssellänge
Für asymmetrische Verfahren wird empfohlen, eine Schlüssellänge von wenigstens 2048 Bit zu verwenden.

BEISPIELE

Eines der bekanntesten asymmetrischen Verschlüsselungsverfahren ist RSA (Verfahren nach Rivest, Shamir und Adleman). Daneben wird heutzutage des Öfteren das Verschlüsselungsverfahren Elgamal (benannt nach seinem Entwickler) eingesetzt.

c) Hybride Verschlüsselungsverfahren
Hybride Verschlüsselungsverfahren (z. B. PGP = Pretty Good Privacy) vereinen die Vorteile der symmetrischen mit den Vorteilen der asymmetrischen Verfahren, ohne jeweils die Nachteile der einen oder anderen mit zu übernehmen. So wird einerseits das Schlüsselverteilungsproblem gelöst und andererseits bleibt der Geschwindigkeitsvorteil der symmetrischen Verschlüsselung erhalten.
Mit hybriden Verfahren können Nachrichten in der Regel
– nur verschlüsselt,
– nur elektronisch signiert oder
– verschlüsselt und elektronisch signiert
werden.

Erzeugung eines Session-Keys
Bei den hybriden Verfahren werden die symmetrischen Verfahren zur Verschlüsselung der Nachricht an sich verwendet. Dabei wird ein zufälliger symmetrischer Schlüssel erstellt, der **„Session-Key"** genannt wird. Mit diesem Session-Key werden die zu schützenden Daten symmetrisch verschlüsselt. Anschließend wird der

7.3 Datenschutz-Folgenabschätzung

Inhaltsverzeichnis

Damit die Datenschutz-Grundverordnung auch bei Verarbeitungsvorgängen, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, beachtet wird, ist der **Verantwortliche** für die Durchführung einer Datenschutz-Folgenabschätzung verantwortlich, mit der insbesondere die Ursache, Art, Besonderheit und Schwere dieses Risikos evaluiert werden. Die Datenschutz-Folgenabschätzung ist somit quasi eine **Risikobewertung**. Dagegen besteht für den **Auftragsverarbeiter** im Rahmen einer entsprechenden Tätigkeit keine Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung. Allerdings muss er den Verantwortlichen gemäß Art. 28 Abs. 4 Buchst. f DSGVO bei der Erstellung einer Datenschutz-Folgenabschätzung **unterstützen**. Gemäß Erwägungsgrund 95 zur Datenschutz-Grundverordnung sollte der Auftragsverarbeiter

tenmissbrauchs wirksam verringern. Überdies sollten solche Regeln und Verfahren den berechtigten Interessen der Strafverfolgungsbehörden in Fällen Rechnung tragen, in denen die Untersuchung der Umstände einer Verletzung des Schutzes personenbezogener Daten durch eine frühzeitige Offenlegung in unnötiger Weise behindert würde (Erwägungsgrund 88 zur Datenschutz-Grundverordnung).
Im Regelfall wird es genügen, die Meldung **in schriftlicher Form oder mittels verschlüsselter E-Mail** zu übersenden. Erfolgt eine Informierung zunächst **telefonisch**, sollte baldmöglichst eine schriftliche Benachrichtigung nachgereicht werden. Dies dient auch der gemäß Art. 33 Abs. 5 bestehenden Dokumentationspflicht.

f) Schrittweise Mitteilung

Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen (Art. 33 Abs. 4 DSGVO). Dies bedeutet, dass weitere Informationen nachgereicht werden können, entbindet aber nicht von der fristgerechten Meldefrist.

g) Verzögerte Abgabe der Meldung

Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine **Begründung für die Verzögerung** beizufügen (Art. 33 Abs. 1 Satz 2 DSGVO).
Falls diese Benachrichtigung nicht binnen 72 Stunden erfolgen kann, müssen in der nachträglichen Meldung die Gründe für die Verzögerung angegeben werden und die Informationen schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden (Satz 3 des Erwägungsgrundes 85 zur Datenschutz-Grundverordnung). Rein persönliche Hinderungsgründe (wie z. B. Urlaub oder Krankheit) des Verantwortlichen begründen keine verzögerte Abgabe der Meldung, da für solche Fälle entsprechende Vertretungsmaßnahmen ergriffen werden müssen.

h) Unterrichtung durch den Auftragsverarbeiter

Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, muss er diese dem Verantwortlichen unverzüglich melden (Art. 33 Abs. 2 DSGVO). Eine Ausnahme von der Meldepflicht gibt es in diesem Fall nicht. Eine Meldung vom Auftragsverarbeiter an die Aufsichtsbehörde ist nicht erforderlich. Allerdings muss der Verantwortliche gegebenenfalls die Aufsichtsbehörde verständigen.
Unterlässt der Auftragsverarbeiter eine unverzügliche Informierung des Verantwortlichen, so drohen ihm gemäß Art. 83 Abs. 4 Buchst. a Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist.