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

Dezember 2015 Ausgabe Nr. 82

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

Am Abend des 15. Dezember ist ein Ereignis eingetroffen, mit dem die Datenschutzgemeinde – auch wir – nicht gerechnet hat. Nach rund vier Jahren Verhandlungsdauer haben sich die Verhandlungsführer des EU-Parlaments, der EU-Kommission und des Ministerrates über den genauen Wortlaut der DS-GVO geeinigt (http://statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf).

Im Anschluss an diese im Trilog erzielte politische Einigung werden die Texte in ihrer endgültigen Fassung Anfang 2016 vom Europäischen Parlament und vom Rat formell angenommen. Nach zwei Jahren – also Anfang 2018 – sind die neuen Vorschriften sodann anzuwenden.

1. Zielsetzung der Reform des Europäischen Datenschutzrechts

Erinnern wir uns kurz daran, was die EU-Kommission eigentlich veranlasst hat, eine Reform des Europäischen Datenschutzrechts in Angriff zu nehmen. Die wichtigsten politischen Ziele der EU-Kommission waren:

- Modernisierung des EU-Rechtsrahmens zum Schutz personenbezogener Daten, insbesondere um den Herausforderungen der Globalisierung und der Nutzung neuer Technologien gerecht zu werden;
- Stärkung der Einzelnenrechte und gleichzeitiges Abbauen von Verwaltungsformalitäten, um den freien Verkehr personenbezogener Daten innerhalb der EU und darüber hinaus zu gewährleisten;
- Verbesserung der Klarheit und Stimmigkeit der EU-Vorschriften zum Schutz personenbezogener Daten, sowie stimmige und wirksame Umsetzung und Anwendung des Grundrechts auf Schutz der persönlichen Daten in allen Tätigkeitsbereichen der Union.

2. Harmonisierung misslungen?

Schon beim ersten kurzen Durchlesen der finalen Fassung ist festzustellen, dass vor allem das letztgenannte Ziel der EU-Kommission, nämlich die Harmonisierung des Europäischen Datenschutzrechts, gründlich misslungen ist. So sind in der Endfassung eine Vielzahl von sogenannten „Öffnungsklauseln“ enthalten, d.h. die EU-Mitgliedstaaten können bei vielen Bestimmungen der DS-GVO von dieser abwei-

chende nationale Regelungen festlegen. Hiezu einige Beispiele:

Art. 6[1] – Rechtmäßigkeit der Verarbeitung

Abs. 2a.: (neu) Die Mitgliedstaaten können spezifischere Vorkehrungen beibehalten oder einführen, um die Anwendung der Regeln dieser Bestimmung in Bezug auf die Verarbeitung personenbezogener Daten zwecks Übereinstimmung mit Art. 6 Abs. 1 Lit. c *[Anm.: Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung]* und e *[Anm.: Verarbeitung zum Schutz lebenswichtiger Interessen]* zu adaptieren, indem sie genauer die spezifischen Erfordernisse der Verarbeitung sowie weitere Maßnahmen zur Sicherung einer gesetzeskonformen und fairen Verarbeitung einschließlich der speziellen Verarbeitungssituationen des Kapitel IX *[Anm.: Meinungsfreiheit, Zugang zu offiziellen Dokumenten, Beschäftigtendaten, Forschung und Statistik, berufliche Verschwiegenheitspflichten, Daten von Religionsgemeinschaften…]* festlegen.

Abs. 3.: Die Rechtsgrundlage für die Verarbeitung gem. Abs. 1 Lit. c und e muss festgelegt werden im Einklang mit

(a) dem Unionsrecht oder

(b) dem nationalen Recht des Mitgliedstaates, dem der für die Verarbeitung Verantwortliche unterliegt.

Art. 8 – Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

Abs. 1.: In den Fällen, in denen Art. 6 Abs. 1 Lit. a *[Anm.: Einwilligung des Betroffenen]* zutrifft, ist bei einem Angebot von Diensten der Informationsgesellschaft, das sich direkt an ein Kind richtet, die Verarbeitung personenbezogener Daten eines Kindes unter 16 Jahren, oder falls das Recht des Mitgliedstaats ein niedrigeres Alter, das nicht unter 13 Jahren liegt, vorsieht, nur dann rechtmäßig, wenn die Zustimmung durch den Träger der elterlichen Verantwortung für das Kind erteilt wird.

Anm.: Die etwas komplizierte Bestimmung hat anfangs zu Missverständnissen geführt, weil einige Experten und Medien meinten, dass hiermit das Mindestalter zur Nutzung von Facebook & Co. auf 16 Jahre angehoben werde. Ursprünglich wollte die EU-Kommission ein EU-Mindestalter von 13 Jahren festlegen, ab dem Jugendliche Onlinedienste wie Facebook u.a. ohne Erlaubnis ihrer Erziehungsberechtigten nutzen dürfen. Dieser Wunsch fand jedoch keine Unterstützer, sind doch die entsprechenden Gesetze der Mitgliedstaaten zu unterschiedlich (selbst innerhalb Österreichs finden sich hierzu Unterschiede je nach Bundesland). Der nun festgelegte Kompromiss erlaubt es den Mitgliedstaaten nunmehr, das Mindestalter zwischen 13 und 16 Jahren zu wählen, darüber oder darunter darf es jedoch nicht liegen.

Art. 9 – Verarbeitung besonderer Datenkategorien

Abs. 2.: Absatz 1 gilt nicht in folgenden Fällen *[Anm.: Abs. 1 enthält so wie Art. 8 Abs. 1 der RL 95/46/EG – umgesetzt in nationales Recht mit § 1 DSG 2000 – ein grundsätzliches Verarbeitungsverbot für sensible Daten, das mit einem in § 9 DSG 2000 enthaltenen taxativen Katalog zulässiger Ausnahmen verknüpft ist]*:

(a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere Zwecke ausdrücklich zugestimmt, außer das Unionsrecht oder das Recht des Mitgliedstaates sehen vor, dass das in Abs. 1 festgelegte Verbot durch die betroffene Person nicht aufgehoben werden kann oder

(b) die Verarbeitung ist erforderlich, damit der für die Verarbeitung Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten oder einem Kollektivvertrag nach dem Recht des Mitgliedstaa-

[1] Anm.: Alle Angaben zur Nummerierung beziehen sich auf die derzeit vorliegende temporäre Fassung. Sie können sich bis zum Erscheinen des offiziellen Enddokuments noch ändern.

tes, das angemessene Garantien für die Grundrechte und Interessen der betroffenen Person vorsieht, zulässig ist.

Anm.: Auch die Buchstaben g, h, hb und i sowie Absatz 4 des Art. 9 sehen die Anwendbarkeit des Rechtes der Mitgliedstaaten vor.

3. Drastische Erhöhung des Bußgeldes

In der Fassung vom 11. Juli 2015, die als Grundlage der Trilog-Verhandlungen diente, waren noch eine Höchststrafe von EUR 1.000.000,- bzw. im Falle eines Unternehmens 2 % des weltweit erzielten Jahresumsatzes des vorhergegangenen Geschäftsjahres vorgesehen. Diese Geldbußen wurden nunmehr drastisch erhöht.

Die Fassung von Juni 2015 unterteilte in Art. 79, der allgemeine Bedingungen für die Verhängung von Bußgeldern definierte, und Art. 79a, in dem diese konkretisiert wurden. Die Inhalte dieser beiden Artikel wurden nun in einem neuen Art. 79 zusammengefasst. Laut diesem kann das Bußgeld bis zu EUR 20.000.000,- betragen. Die Strafhöhe ist zusätzlich nach oben hin offen, denn das Strafhöchstausmaß kann bis zu 4 % des weltweiten Konzernumsatzes betragen. Diese Höchststrafe – ursprünglich gegen die globalen Internetkonzerne wie Facebook & Co. gerichtet – kann nunmehr jede Firma treffen, also auch KMUs. Die ursprünglich für diese Unternehmensgröße vorgesehenen Erleichterungen sind in der finalen Fassung der DS-GVO nicht mehr enthalten.

4. Klarheit und Stimmigkeit?

Was die versprochene Klarheit anbelangt, wird die vorliegende DS-GVO diesem Anspruch nur zum Teil gerecht. Zwar werden verschiedene Anliegen und Konfliktpunkte der jüngeren Zeit umfassend geregelt, das betrifft aber vor allem jene Bereiche, zu denen sich bereits sehr konkrete Handlungsanweisungen herauskristallisiert hatten, die nunmehr vollständig in Unionsrecht gefasst wurden. Wichtige Zukunftsthemen – allen voran der datenschutzkonforme Umgang mit „Big Data“ – bleiben unscharf und werden auf wenig zufriedenstellende Weise behandelt.

Der vorliegenden Datenschutzgrundverordnung kann man somit auch den Vorwurf der Anlassbezogenheit nicht ersparen. Sie zielt stark auf aktuelle Problemlagen ab, während ein umfassender Ausblick in die Zukunft fehlt. Es bleibt abzuwarten, ob die DS-GVO auch nur annähernd so gut altert wie die inzwischen über 20 Jahre alte Richtlinie 95/46/EG.

Klärungen finden sich insbesondere beim Datenschutz im Internetverkehr, der ja ein besonderes Anliegen der Initiatoren der DS-GVO darstellte. Hier sind unter anderem folgende neue Regelungen zu finden:

- In Art. 4 Abs. 1 wird die Definition der personenbezogenen Daten um Online-IDs und Standortdaten erweitert.
- In Art. 23 wird Auftraggebern Datenschutz „by design“ und „by default“ vorgeschrieben (Art. 23). Auftraggeber müssen demnach bereits beim Entwurf ihrer Produkte Datenminimierung und ähnliche Datenschutzmaßnahmen vorsehen.
- In Art. 7 Abs. 4 wird geregelt, dass die Zustimmung zur Datenverwendung nicht zur Voraussetzung eines Vertrags oder eines Dienstes gemacht werden darf, sofern sie nicht zur Vertragserfüllung tatsächlich notwendig ist. Die Nutzung z.B. eines Dienstes darf also nicht von der Zustimmung zur Preisgabe personenbezogener Daten abhängig gemacht werden, es sei denn, das ist für die Bereitstellung unbedingt erforderlich.
- In Art. 3 Abs. 2b wird klar festgelegt, dass auch das Monitoring von Betroffenen in-

nerhalb der EU in den Anwendungsbereich der neuen DS-GVO fällt.

Eine ganze Reihe neuer Bestimmungen also, die viele Fragestellungen, die zuletzt im Zusammenhang mit Cookies, Online-Profiling und zielgruppenorientierter Werbung auftraten, abschließend klären sollten. Viele dieser Ansätze waren bereits an verschiedener Stelle behandelt worden; nun wurden sie in rechtliche Bestimmungen übernommen.

Deutlich weniger detailliert ist dagegen die Behandlung des Themas „Big Data". Hier scheinen sich einerseits die Wünsche der Lobbyisten, andererseits auch die hohen Erwartungen, die seitens der Politik an diese Verarbeitungsform geknüpft werden, durchgesetzt zu haben. Möglicherweise liegt die mangelhafte Behandlung aber auch daran, dass immer noch keine überzeugenden Grundregeln eines datenschutzgerechten Umgangs mit dieser Thematik erkennbar sind.

Die DS-GVO bringt hier jedenfalls kaum Klärung. Generell sind wenige Bestimmungen zu finden, die sich auf Big Data beziehen lassen. Abgesehen vom neuen Prinzip der „Transparenz" gegenüber den Betroffenen, das auch als Forderung nach Offenlegung der Verwendungszwecke und Methoden der Datenverarbeitung gegenüber den Betroffenen zu interpretieren ist, sowie einigen Ausnahmebestimmungen für öffentliches Gesundheitswesen und Forschung sticht nur Art. 6 Abs. 3a heraus.

Dieser behandelt die Prüfpflicht, der ein Auftraggeber unterliegt, sofern er Daten zu anderen als den ursprünglichen Zwecken verarbeiten will – die typische Big Data-Problematik also. Laut DS-GVO ist dabei unter anderem vom Auftraggeber in Betracht zu ziehen, ob eine Verbindung zwischen diesen Verwendungszwecken besteht, ob dabei auch sensible Daten verarbeitet werden und welche Konsequenzen sich daraus für den Betroffenen ergeben könnten. Detailliertere Erläuterungen und Anhaltspunkte für die Abschätzung, vielleicht auch die optionale oder obligatorische Einschaltung nationaler Datenschutzbehörden zu Begutachtungs- oder Genehmigungszwecken, wären hilfreich gewesen und würden den Auftraggebern erlauben, die Rechtmäßigkeit ihrer Verarbeitungen rechtzeitig und ohne Risiko der Bestrafung abzuklären.

Man kann nur hoffen, dass bis zum Inkrafttreten der DS-GVO bessere Anhaltspunkte vorliegen, wie diese Abschätzung im Detail aussehen soll. Klarheit, was erlaubt und was unzulässig ist, wurde in diesem Bereich jedenfalls nicht hergestellt.

Wir werden in den nächsten Monaten die durch die DS-GVO entstehenden Veränderungen im Detail auswerten und Ihnen darüber berichten. Vorerst bleibt abzuwarten, wie die konsolidierte Fassung in der deutschen Übersetzung ausfallen wird.

••••