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

Juni 2012 Ausgabe Nr. 68/69

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

Wie wir Sie bereits in unserer Ausgabe Nr. 66 / 67 informiert haben, hat die Europäische Kommission im Jänner dieses Jahres einen Entwurf für ein Gesamtkonzept für den Datenschutz in der EU verfasst.

Die zuständige EU-Justizkommissarin und Vizepräsidentin der EU-Kommission, Viviane Reding, ließ den Entwurf mit der Bezeichnung „Vorschlag für VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR) {SEK(2012) 72 endgültig} {SEK(2012) 73 endgültig}" („Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)") am 25. Jänner 2012 veröffentlichen.

Grund für eine solche Verordnung sind die neuen vielfältigen Herausforderungen für den Datenschutz, in erster Linie bedingt durch die Dynamik iZm Internetanwendungen mitsamt den modernen Technologien wie soziale Netzwerke oder Cloud Computing. Die Verordnung verfolgt Lösungsansätze und gibt Ziele vor, um die bestehenden Datenschutzvorschriften entsprechend zu ändern und auf die heutigen datenschutzrechtlichen Anforderungen anzupassen. Die Europäische Datenschutzverordnung soll an die Stelle der Richtlinie 95/46/EG treten, wobei die wohl die wichtigste Änderung in der Tatsache liegt, dass anstelle einer Richtlinie nunmehr eine Verordnung vorliegt.

***Richtlinien** sind gem. Art. 288 Abs. 3 EG-Vertrag für jeden Mitgliedstaat, an den sie gerichtet sind, **nur** hinsichtlich des zu erreichenden Zieles verbindlich, während die Wahl der Form und der Mittel den innerstaatlichen Stellen überlassen bleibt.*

***Verordnungen** gem. Art. 288 Abs. 2 EG-Vertrag haben dagegen allgemeine Geltung und sind in allen Teilen verbindlich und gelten unmittelbar in jedem Mitgliedstaat.*

Datenschützer wie auch Arbeitnehmervertreter, etwa AK und GPA, äußern am gegenständlichen Entwurf erste Kritik. Die Secur-Data nahm am 24. April an der AK Informationsveranstaltung „Die neue Europäische Datenschutzverordnung" teil und hält für Sie die wichtigsten Kritikpunkte weiter unten fest.

Weiters greifen wir in dieser Ausgabe die letzten beiden Novellierungen des TKG 2003 auf. Diese umfassen die Vorratsdatenspeicherung, welche auf der EU-Richtlinie 2006/24/EG beruht und die seit 1. April 2012 von Telekommunikationsbetreibern vorzunehmen ist, sowie Verbesserungen für Telekommunikationskunden wie z.B. Vertrags- und Kostentransparenz und in Bezug auf den Datenschutz.

Die Secur-Data hat für Sie die wichtigsten Neuigkeiten zusammengefasst.

AK Informationsveranstaltung
„Die neue Europäische Datenschutzverordnung“

Zur Veranstaltung

Vor dem Hintergrund des weiter oben genannten Verordnungsentwurfes für ein Gesamtkonzept für den Datenschutz in der EU fand am 24. April 2012 im AK Bildungszentrum in Wien 4, Theresianumgasse 16-18, die Veranstaltung „Die neue Europäische Datenschutzverordnung“ statt.

Die Abgeordnete des Europäischen Parlaments und stellvertretende Vorsitzende im Ausschuss für Recht, Evelyn Regner, referierte über die aktuelle Datenschutz-Diskussion im Europäischen Parlament.

Gerda Heilegger von der AK Wien, Abteilung Sozialpolitik, trug zu rechtlichen Aspekten rund um die Arbeitnehmerbelange vor. Im Rahmen der Veranstaltung fand eine Diskussion statt, an der u. a. Joe Weidenholzer, Abgeordneter des Europäischen Parlaments und Mitglied im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres, teilnahm.

Wir haben nachstehend die wichtigsten genannten Kritikpunkte am gegenständlichen Verordnungsentwurf für Sie festgehalten.

Kritikpunkte

1. Der betriebliche Datenschutzbeauftragte

Im Entwurf der Datenschutzverordnung ist die Einrichtung eines betrieblichen Datenschutzbeauftragten für Betriebe mit einer Größe von 250 oder mehr Mitarbeitern verpflichtend vorgesehen, sofern im Betrieb personenbezogene Daten verarbeitet werden.

Weil ca. 99 % der Unternehmen in Österreich weniger als 250 Mitarbeiter beschäftigen, kritisieren Regner und Weidenholzer, dass diese Grenze viel zu hoch liegt, da dadurch die Mehrheit der Unternehmen und deren Beschäftigte schlechter gestellt werden. Daher schlagen Regner und Weidenholzer eine Grenze von 50 Mitarbeitern vor. In Österreich besteht bekanntlich derzeit keine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten.

Im Vergleich dazu ist derzeit in Deutschland gem. § 4f Abs. 1 BDSG (Bundesdatenschutzgesetz) ein Beauftragter für den Datenschutz im nicht-öffentlichen Bereich dann zu bestellen, wenn mehr als 9 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. In diesem Kontext lassen sich die Bestimmung des Verordnungsentwurfes in Deutschland als erhebliche Verschlechterung des Datenschutzes einstufen. Kritisiert wird, dass für den Fall einer solchen Verschlechterung in der Verordnung keine Regelungen vorgesehen sind.

Weiters kritisieren die Abgeordneten, dass der gegenständliche Verordnungsentwurf keine konkreten Befugnisse des betrieblichen Datenschutzbeauftragten definiert und dessen Mindestausbildung nicht festlegt.

2. Das one-stop-shop-Prinzip

Der Verordnungsentwurf sieht vor, dass die Datenschutzbehörde jenes Landes für ein Unternehmen zuständig ist, in dem sich die Hauptniederlassung befindet – etwa die Kon-

zernzentrale. Nach dem one-stop-shop-Prinzip ist diese für das gesamte Unternehmen, d.h. auch Niederlassungen bzw. Konzernunternehmen in anderen EU-Mitgliedstaaten zuständig. Dem sollen insbesondere Kooperationsvereinbarungen zwischen den einzelnen Datenschutzbehörden zugrunde liegen.

Regner und Weidenholzer kritisieren, dass dadurch insbesondere große Unternehmen die Möglichkeit haben, ihren Hauptsitz in einen EU-Mitgliedstaat zu legen, in dem die verfügbaren Ressourcen der Datenschutzbehörden ein weniger rasches Entscheiden und Handeln erwarten lassen.

Zudem wird von den Kritikern höherer Administrationsaufwand auf Seite der Datenschutzbehörden vermutet, da die Datenschutzbehörden in einem Land nun die Anlaufstelle auch für Belange aus den anderen Mitgliedstaten sind.

Wie die Rechtsdurchsetzung innerhalb dieses one-stop-shop-Konzeptes in der Praxis erfolgen soll, ist nach Meinung der Abgeordneten eine offene Frage, wobei die Zusammenarbeit und der Austausch unter den Datenschutzbehörden nur relativ abstrakt geregelt sind und rechtlich „zerfließen“. Heilegger befürchtet in diesem Kontext Verzögerungen im Ablauf, Verteuerungen und verschlechterte Rechtsdurchsetzung.

3. Sonstige Kritik

Heilegger kritisiert, dass der Verordnungsentwurf keine Meldung bzw. Publizität von Datenanwendungen bei einem Register vorsieht, so wie es derzeit durch das DSG 2000 geregelt ist. Dadurch hätten u.a. Betriebsräte keine Möglichkeit mehr, bei der Behörde Informationen über Datenanwendungen einzuholen, um diese etwa iZm Arbeitnehmerbelangen zu prüfen.

Weiters kritisiert Heilegger das vorgesehene Konzernprivileg. Durch dieses sollen Übermittlungen an Konzernunternehmen zulässig sein, sobald der Auftraggeber einseitig eine entsprechende Richtlinie in der Organisation verankert hat.

Regner und Weidenholzer kritisieren auch die hohe Anzahl von delegierten Rechtsakten, die als Ausführungsverordnungen vorgesehen sind (Sonder-Verwaltungsverfahren nach der EU-VO), deren Notwendigkeit es zu hinterfragen gilt. Einerseits werden dadurch sowohl Komplexität als auch Aufwand erhöht, andererseits leidet darunter die Transparenz.

Ausblick

Während der vorliegende Vorschlag von allen 27 EU-Mitgliedstaaten akzeptiert werden muss, sind noch viele Fragen offen, weshalb eine rasche Umsetzung nicht zu erwarten ist.

Datenschutzexperten rechnen mit etwa 2 bis 3 Jahren, bis die Mitgliedstaaten die Verordnung annehmen, sofern keine größeren Änderungen vorgenommen werden, die diese Dauer erstrecken.

Wir werden Sie jedenfalls in dieser Angelegenheit auf dem Laufenden halten.

Novellierung des TKG 2003 (Telekommunikationsgesetz 2003)

Zur Novellierung

Mit dem Bundesgesetzblatt BGBl. I Nr. 102/2011 vom 21. November 2011 nahm der Gesetzgeber wesentliche Änderungen des TKG 2003 vor. So werden etwa dem Telekommunikationskunden mehr Rechte eingeräumt – insbesondere Informationsrechte, höhere Trans-

parenz und Schutz vor überhöhten Telekommunikationsrechnungen. Darüber hinaus enthält diese Novelle auch Verbesserungen im Bereich des Datenschutzes für die Nutzer, die von allen „Diensten der Informationsgesellschaft“ zu gewährleisten sind. Die wichtigste Verbesserung betrifft die Verwendung von „Cookies“. Damit werden die als „Telekomreformpaket“ der EU bezeichneten Richtlinien 2009/140/EG zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste, weiters die Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und die Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste (Rahmenrichtlinie) sowie 2009/136/EG zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und die Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz umgesetzt. Weiters werden mit dieser Novelle die erforderlichen begleitenden Regelungen zur Verordnung (EG) Nr. 1201/2009 zur Einrichtung des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) und des Büros erlassen.

Im Zuge der Novelle erlangt auch die RTR (Rundfunk und Telekom Regulierungs-GmbH) mehr Rechte. So verfügt diese nun über das Recht, mittels Verordnung den Detaillierungsgrad, Inhalte sowie die Form der Inhalte in Bezug auf Telekommunikationsverträge und Änderungen von Verträgen (einschließlich AGB) zu bestimmen.

Weiters hat der Gesetzgeber mit dem Bundesgesetzblatt BGBl. I Nr. 27/2011 vom 18. Mai 2011 die mit 1. April 2012 in Kraft getretene und viel diskutierte Vorratsdatenspeicherung erlassen. Damit wird die EU-Richtlinie 2006/24/EG über die „Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden“ in nationales Recht umgesetzt. Die Vorratsdatenspeicherung schreibt den Betreibern vor, die in § 102a TKG 2003 bestimmten Daten aus dem Telekommunikationssystem, darunter Daten betreffend die Nutzung eines Dienstes, für die Dauer von sechs Monaten zu speichern.

An dieser Stelle greifen wir für Sie die wesentlichsten Änderungen der beiden Novellen auf.

Änderungen

Verkürzte Mindestvertragsdauer

Die anfängliche Mindestvertragsdauer für Kommunikationsdienste mit Verbrauchern (z.B. Mobilfunkvertrag) ist nun gem. § 25d Abs. 1 TKG 2003 (Mindestvertragsdauer) auf max. 24 Monate beschränkt. Höhere Bindefristen sind somit unzulässig.

Bessere Informationen vor Vertragsabschluss

Gem. § 25b TKG 2003 (Besondere Informationspflichten) hat der Betreiber von öffentlichen Kommunikationsdiensten (Provider) vor dem Vertragsabschluss über die wesentlichen Merkmale des Vertrages iSv § 25 Abs. 4 und 5 TKG 2003 in klarer Form zu informieren bzw. die Informationen zugänglich zu machen. § 25 Abs. 4 und 5 TKG 2003 geben die Mindestinhalte der Allgemeine Geschäftsbedingungen und der Entgeltbestimmungen vor, wozu etwa folgende Inhalte zählen: „Information über die Möglichkeiten der Rufnummernanzeige und Unterdrückung“, „Informationen über Einschränkungen im Hinblick auf den Zugang zu oder die Nutzung von Diensten“, „zugesicherte Dienstqualität“, „Informationen über vom Unternehmen zur Messung und Kontrolle des Datenverkehrs eingerichteten Verfahren“, „Arten der angebotenen Wartungsdienste und

der verfügbaren Kundendienste“, „alle vom Betreiber auferlegten Beschränkungen für die Nutzung der von ihm zur Verfügung gestellten Endeinrichtungen“, „sofern eine Verpflichtung nach § 69 Abs. 2 TKG 2003 besteht, die Möglichkeit des Teilnehmers sich zu entscheiden, ob seine personenbezogenen Daten in ein Teilnehmerverzeichnis aufgenommen werden sollen und gegebenenfalls die betreffenden Daten“, „Bestimmungen über die Intervalle der periodischen Rechnungslegung, die drei Monate nicht überschreiten dürfen“ und „Einzelheiten über einmalige, regelmäßig wiederkehrende und variable Entgelte“. Zudem hat die RTR in diesem Kontext nun das Recht, mittels Verordnung den Detaillierungsgrad, Inhalte sowie die Form der Inhalte zu bestimmen.

Bessere Information bei Vertragsänderungen

Gem. § 25 Abs. 2 bis 3 TKG 2003 ist der „wesentliche Inhalt [..] nicht ausschließlich begünstigender Änderungen“ der AGB (Allgemeine Geschäftsbedingungen) oder von Entgelten dem Teilnehmer mindestens einen Monat vor Inkrafttreten schriftlich mitzuteilen, wie etwa durch ein eigenes Schreiben oder auf der Rechnung. Auch hier hat die RTR nun das Recht, mittels Verordnung den Detaillierungsgrad, Inhalte sowie die Form der Inhalte zu bestimmen.

Datendienste-Sicherheitssperre eingeführt

Gem. § 29 Abs. 2 TKG 2003 können neben Mehrwertnummern nun auch Datendienste gesperrt werden. Die Sperre hat einmal pro Jahr entgeltfrei möglich zu sein.

Rechnungseinspruchs-Frist verlängert

Gem. § 71 Abs. 1 bis 1a TKG 2003 hat ein Teilnehmer, sofern dieser die Richtigkeit der ihm verrechneten Entgelte für einen Kommunikationsdienst bezweifelt, nun eine Frist von drei Monaten, um gegen eine Rechnung des Telekommunikationsdienstanbieters schriftlich Einspruch zu erheben.

Wahlrecht auf Rechnung in Papierform oder elektronischer Form

§ 100 Abs. 1 TKG 2003 räumt dem Teilnehmer bei Vertragsabschluss das Recht ein, zwischen einer Rechnung in elektronischer oder Papierform zu wählen. Die Ausstellung der Rechnungen in Papierform hat unentgeltlich zu erfolgen und darf vertraglich nicht ausgeschlossen werden. Erfolgt der Einzelentgeltnachweis in elektronischer Form, so hat der Teilnehmer das Recht, diesen auf gesondertes Verlangen entgeltfrei in Papierform zu erhalten.

Kostenkontrolle als Schutz vor hohen Telekommunikationsrechnungen

In § 25a TKG 2003 wird die Kostenbeschränkung geregelt. Gem. § 25a Abs. 1 TKG 2003 ist die Regulierungsbehörde befugt, den Telekommunikationsbetreibern mittels Verordnung Verpflichtungen iZm der Bereitstellung von Möglichkeiten der Kostenkontrolle iSv Kostentransparenz aufzuerlegen. Gem. § 25a Abs. 2 TKG 2003 kann die Regulierungsbehörde etwa folgende Aspekte regeln:

- Detaillierungsgrad und Form der Einrichtungen zur Kostenbeschränkung bzw. Kontrolle
- Schwellenwerte, ab denen z.B. unentgeltliche Warnhinweise über den Verbrauch von vertraglichen Freieinheiten zu erfolgen haben
- Einrichtung kostenfreier Dienste-Sperren bei ungewöhnlichen oder übermäßigen Verbraucherverhalten

Die Regulierungsbehörde hat währenddessen die technischen Möglichkeiten sowie die Art des Teilnehmerverhältnisses und des Dienstes insofern zu berücksichtigen, dass die Teilnehmer die Möglichkeit haben, ihre Ausgaben zu kontrollieren und zu steuern. Das Ziel ist es, die Verbraucher vor übermäßigem Entgeltanfall zuverlässig zu schützen.

Datensicherheitsmaßnahmen

§ 95 Abs. 1 und 3 TKG 2003 verpflichtet jeden Betreiber eines öffentlichen Kommunikationsdienstes zur Erlassung von Datensicherheitsmaßnahmen iSd § 14 DSG 2000, sowie gem. Abs. 2 den Nutzer bei Bestehen eines besonderen Risikos der Verletzung der Vertraulichkeit sowie über mögliche Maßnahmen zur Risikominimierung inkl. der damit verbundenen Kosten zu informieren.

Sicherheitsverletzungen

§ 95a TKG 2003 enthält Regelungen in Bezug auf die sogenannte „Data Breach Notification Duty", so wie sie auch im § 24 Abs. 2a DSG 2000 enthalten ist.

Datenschutz – Allgemeines

Die wohl wichtigste Datenschutzbestimmung des § 96 TKG 2003 ist die in Abs. 3 enthaltene Forderung, wonach die Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten nur dann zulässig ist, wenn der Teilnehmer oder der Nutzer (= Betroffene iSd § 4 Z 3 DSG 2000) seine Einwilligung dazu erteilt hat. Diese Regelung betrifft grundsätzlich auch die sogenannten „Cookies". Diese Bestimmung betrifft vor allem jene Unternehmen – vor allem aus der Werbewirtschaft –, die Internetverkehrsdaten zum Zwecke des „Behavioral Targeting" für User Tracking verwenden. Erwägungsgrund 66 der Richtlinie 2009/136/EG (als E-Privacy- oder auch als Cookie-Richtlinie bezeichnet) enthält jedoch im vorletzten Absatz folgende Bestimmung: *„Wenn es technisch durchführbar und wirksam ist, kann die Einwilligung des Nutzers zur Verarbeitung im Einklang mit den entsprechenden Bestimmungen der Richtlinie 95/46/EG über die Handhabung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung ausgedrückt werden".*

Diese Formulierung wurde trotz Intervention der WKÖ allerdings in den § 96 Abs. 3 nicht übernommen, findet sich jedoch – fast wortgleich – in den Erläuterungen zu diesem Paragraph, und zwar: *„Wenn dies technisch durchführbar ist, kann die Einwilligung des Nutzers zur Verarbeitung über die Handhabung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung ausgedrückt werden"*. Daraus kann abgeleitet werden, dass ein Nutzer, der in seinen Browsereinstellungen das Setzen von Cookies zulässt, die erforderliche Einwilligung erteilt. Will der Nutzer keine Cookies mehr akzeptieren, so kann er ja jederzeit die Einstellungen entsprechend anpassen. Diese Auslegung ist allerdings in Datenschutzkreisen nicht unstrittig.

Vorratsdatenspeicherung

Gem. § 102a TKG 2003 sind Provider (Anbieter öffentlicher Kommunikationsdienste) zur verdachtsunabhängigen Speicherung von Vorratsdaten für die Dauer von sechs Monaten verpflichtet. Der ausschließliche Zweck liegt in der Ermittlung, Feststellung und Verfolgung von Straftaten. Die Speicherpflicht betrifft gem. § 102a Abs. 5 TKG 2003 „nur [..] jene Daten [die] gemäß Abs. 2 bis 4, [..] im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet werden".

Folgende Daten haben die Provider gem. § 102a Abs. 2 bis 4 TKG 2003 iZm den genannten Diensten auf Vorrat zu speichern:

Internet-Zugangsdienste

Gem. § 102a Abs. 2 TKG 2003 obliegt Providern von Internet-Zugangsdiensten unter anderem die Speicherung folgender Daten:

- Name, Anschrift und Teilnehmerkennung des Teilnehmers
- Datum und Uhrzeit der Zuteilung und des Entzugs einer öffentlichen IP-Adresse

- bei Internetzugang mittels Wählanschluss (dial up): Rufnummer des anrufenden Anschlusses
- eindeutige Kennung des Anschlusses, über den der Internet-Zugang erfolgt

Öffentliche Telefondienste einschließlich Internet-Telefondienste

Gem. § 102a Abs. 3 TKG 2003 obliegt Providern von öffentlichen Telefondiensten unter anderem die Speicherung folgender Daten:

- Teilnehmernummer oder andere Kennung des anrufenden und des angerufenen Anschlusses
- Teilnehmernummer, an die ein Anruf umgeleitet wird
- Name und Anschrift des anrufenden und des angerufenen Teilnehmers
- Beginn und Dauer eines Kommunikationsvorganges
- Art des Dienstes (Anrufe, Zusatzdienste und Mitteilungs- und Multimediadienste)
- Mobilteilnehmerkennung (IMSI) des anrufenden und des angerufenen Anschlusses
- Mobilfunkgerätekennung (IMEI) des anrufenden und des angerufenen Anschlusses
- Standortkennung (Cell-ID) bei Beginn einer Verbindung

Unter „andere Kennung“ fällt etwa die teilnehmerbezogene IP-Adresse oder SIP-Adresse.

Der Begriff „Anrufe“ inkludiert Sprachtelefonie, Sprachspeicherdienst, Konferenzschaltungen und Datenabrufungen.

„Zusatzdienste“ schließt Rufweiterleitung und Rufumleitung ein.

Der Begriff „Mitteilungsdienste und Multimediadienste“ umfasst auch Kurznachrichtendienste (SMS) sowie erweiterte Nachrichtendienste (EMS) und Multimediadienste (MMS).

E-Mail-Dienste

Gem. § 102a Abs. 4 TKG 2003 obliegt Providern von E-Mail-Diensten unter anderem die Speicherung folgender Daten:

- Teilnehmerkennung, die dem Teilnehmer zugewiesen ist
- Name und Anschrift des Teilnehmers
- bei E-Mail-Versand: E-Mail-Adresse und die öffentliche IP-Adresse des Absenders sowie die E-Mail-Adresse eines jeden Empfängers
- bei E-Mail-Empfang: E-Mail-Adresse des Absenders und des Empfängers der Nachricht sowie die öffentliche IP-Adresse der letztübermittelnden Kommunikationsnetzeinrichtung
- bei An- und Abmeldung beim E-Mail-Dienst: Datum, Uhrzeit, Teilnehmerkennung und öffentliche IP-Adresse

Unter „Anmeldung bzw. Abmeldung bei einem E-Mail Dienst“ sind zu verstehen:

- Login / Logout bei einem Webmaildienst
- Userauthentifizierung beim Zugriff auf das Postfach (z.B. via IMAP oder POP)

Sonstiges, Erläuterungen

Hinsichtlich der Speicherdauer sieht die RL 2006/24/EG eine Frist von min. sechs Monaten und max. zwei Jahren ab dem Zeitpunkt des Kommunikationsvorganges vor. Der österreichische Gesetzgeber hat sich mit einer Aufbewahrungsdauer von sechs Monate somit für die Umsetzung des Mindestmaßes entschieden.

Betreffend die IP-Adresse trifft die Speicherpflicht jenen Internet Access Provider, dem die Verwaltung der öffentlichen IP-Adressen von den IP-Adressverwaltungsinstitutionen (für Europa ist dies RIPE NCC) zugewiesen ist.

Die Speicherpflicht bezieht sich nur auf zugewiesene öffentliche IP-Adressen, nicht aber auf interne Adressen (etwa gem. RFC 1918, RFC 1631, RFC 2663, RFC 3022).

Die Speicherpflicht betrifft jene Daten, die vom jeweiligen Betreiber für die Erbringung seiner eigenen Dienste erzeugt bzw. verarbeitet werden. Bei den auf Vorrat zu speichernden Daten handelt es sich um solche, die beim Kommunikationsdienste-Betreiber bereits vorhanden sind – mit Hilfe oder ohne Hilfe automationsunterstützter Verfahren. Der reine Durchlauf von Daten ist hierbei nicht gemeint, da dies im Sinne der RL 2006/24/EG weder unter das Erzeugen noch Verarbeiten von Daten fällt. Unter reines Durchführen fällt etwa der Betrieb eines MPLS (Multiprotocol Label Switching) Netzwerkes.

Ausgenommen von der Speicherpflicht sind Spam-E-Mails, die vom Betreiber vor der Zustellung in ein Postfach herausgefiltert werden, da hierbei kein vollständiger Kommunikationsvorgang stattfindet. Wird das Spam-E-Mail allerdings in das Empfänger-Postfach zugestellt, gilt die Speicherpflicht.

Ausgenommen von der Speicherpflicht sind gem. § 102a Abs. 6 TKG 2003 Anbieter, die iSv § 34 KOG (KommAustria-Gesetz) als kleine Anbieter einzustufen sind, da für diese die Investition in ein entsprechendes Speichersystem unverhältnismäßig hoch wäre.

Die Speicherpflicht betrifft auch nicht die Inhalte der Kommunikation, wie E-Mail-Inhalt oder aufgerufene Webseites. Erfasst werden aber die Betreffzeile des E-Mails und bestimmte Informationen zu Newsgroup-Diensten oder Chaträumen, wie z.B. IRC-Channels.

Ab dem Ende der sechsmonatigen Speicherpflicht hat der Betreiber gem. § 102a Abs. 8 TKG 2003 innerhalb von einen Monat die Vorratsdaten zu löschen, sofern keine gesetzlichen Aufbewahrungspflichten bestehen (z.B. Ermittlungsverfahren).

Pro und Contra

Während der Staat mit der Vorratsdatenspeicherung über ein Werkzeug zur Verfolgung bzw. Prävention von Kriminalität verfügt, kritisieren Datenschützer, dass durch Missbrauch der Daten Bewegungsabläufe, Bekanntschaften-Profile und Interessensprofile von Menschen möglich sind, was als Eingriff in die Privatsphäre einzustufen ist. Bereits die theoretische Möglichkeit einer zweckfremden Verwendung sehen viele Datenschützer als einen solchen Eingriff.

Zudem werden die Investitionskosten für die Speicherung kritisiert, die für die Provider anfallen.

Die Befürworter der Vorratsdatenspeicherung betonen, dass für die Verfolgung von Internetkriminalität, wie etwa Datendiebstahl, Verbreitung illegaler Inhalte oder Urheberrechtsverletzungen, klassische Ermittlungsinstrumente nicht ausreichen.

Die deutsche SPD hebt hervor, dass die Vorratsdatenspeicherung auch ein erforderliches Mittel zur Verfolgung von Telefonbetrügern ist (z.B. „Enkeltrickbetrüger“).

In diesem Sinne lässt sich hoffen, dass die Vorratsdaten ausschließlich zu ihrem bestimmten Zweck, der Straffverfolgung, verwendet werden und zu einer höheren Aufklärungsquote beitragen.

Jedenfalls hat Österreich mit der Novellierung des TKG 2003 der Umsetzungspflicht der EU-Richtlinie 2006/24/EG Folge geleistet. Ob die Bestimmungen der Richtlinie aufgrund der anhaltenden Diskussion zwischen Befürwortern und Gegnern künftig abgeändert werden, bleibt abzuwarten. Die Secur-Data hält Sie auf dem Laufenden.

••••