nucmag.com

atw

International Journal
for Nuclear Power

2018

5

285
Security Controls for Nuclear Safety

ISSN · 1431-5254
24.– €

Acknowledgments

Some of the addressed modelling and cybersecurity related topics are being elaborated as part of *AREVA GmbH's* (today *Framatome GmbH*) participation in the "SMARTEST" R&D (2015-2018) with German University partners, partially funded by *German Ministry BMWi*.

References

[1] M. Holt, A. Andrews, *Nuclear Power Plant Security and Vulnerabilities,* Congressional Research Service. (n.d.).

[2] IEC 62859:2016, *NPPs – I&C Systems – Requirements for Coordinating Safety and Cybersecurity.*

[3] IEC 61513:2011, *NPPs – I&C Important to Safety – General Requirement for Systems.*

[4] K. Waedt, Y. Ding: 2015, *Safety and Cybersecurity Aspects in the Safety I&C Design for Nuclear Power Plants,* 3rd China (International) Conference on Nuclear Power I&C Technology, Shanghai.

[5] ISO/IEC 27005:2011 – *Information Technology – Security Techniques – Information Security Risk Management.*

[6] M. Parekh, K. Waedt, A. Ciriello, Y. Gao: 2016, *Cybersecurity During Plant Operation,* 42nd Annual Meeting of the SNE, Santander.

[7] IEC 63096 (Draft): 2016, *Security Controls.*

[8] IEC 62645:2014, *NPPs – I&C Systems – Requirements for Security Programmes for Computer-Based Systems.*

[9] IEC 61513:2011 – *NPPs – I&C important to safety – General req. for systems.*

[10] E. Bajramovic, D.Gupta: 2016, *Providing Security Assurance in Line with National DBT Assumptions,* Women in Nuclear (WiN), Shah Alam, Malaysia.

[11] P. Zavarsky, K. Waedt, A. Kuskov: 2015, *High Assurance Cybersecurity Controls against Persistent and Targeted Attacks on Instrumentation and Control Systems in Nuclear Facilities,* 9th International Conference on Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies (NPIC & HMIT 2015), Charlotte, USA.

[12] D. Kushner: 2013, *The Real Story of Stuxnet,* IEEE Spectrum.

[13] IAEA NSS 8:2008, Nuclear Security Series No. 8, Technical Guidance, *Preventive and Protective Measures Against Insider Threats.*

[14] A. Scott, 2015, *Tactical Data Diodes in IACS,* SANS Institute.

[15] E. Bajramovic, J. Bochtler, I. B. Zid, A. Lainer, 2016, *Planning the Selection and Assignment of Security Forensics Countermeasures,* ICONE; Shanghai.

[16] J. Li, E. Bajramovic, Y. Gao, M. Parekh, 2016, *Graded Security Forensics Readiness for SCADA Systems,* GI 2016, Klagenfurt.

[17] E. Knapp, J. Langill: 2014, *Security Monitoring of Industrial Control Systems,* In Industrial Network Security. 2nd Edition, Syngress Publishing.

[18] K. Waedt, A. Kuskov, P. Zavarsky: 2015, *Domain Specific Cybersecurity Applied to I&C,* IAEA, Vienna.

[19] ISO/IEC 27002:2013 *Information Technology – Security techniques – Code of Practice for Information Security Controls.*

[20] Y. Gao, X. Xie, M. Parekh, E. Bajramovic: 2016, *SIEM: Policy-Based Monitoring of SCADA System,* GI 2016, Klagenfurt.

Authors Deeksha Gupta
Karl Waedt
Framatome GmbH
ICPGOP
Henri-Dunant-Straße 50
91058 Erlangen, Germany

Yuan Gao
Framatome GmbH and
Otto-von-Guericke-Universität Magdeburg,
Germany

EU-Datenschutzgrundverordnung – Was bis zum 25.5.2018 beachtet sein muss(te)

Stefan Loubichi

Mit der Datenschutzgrundverordnung (DSGVO) der Europäischen Union beginnt in ein neues Kapitel in der Geschichte des Datenschutzes. Zum 25. Mai 2018 werden wir in der Europäischen Union eine Harmonisierung der Datenschutzbestimmung vorfinden. Mit Geldbußen von bis zu 20 Millionen Euro und Freiheitsstrafen von bis zu 3 Jahren werden die Datenschutzbestimmungen in Zukunft einen hohen Stellenwert haben.

In diesem Aufsatz werden erst einmal Gegenstand und Ziele, sachlicher und räumlicher Anwendungsbereich sowie die Grundsätze für die Verarbeitung personenbezogener Daten vorgestellt.

In der neuen DSGVO wurden die Rechte der betroffenen Personen präzisiert. Dies wird ebenso vorgestellt wie die zusätzlichen Pflichten von Verantwortlichen und Auftragsverarbeitern.

Neue Regelungen in Bezug auf:

- den Datenschutzbeauftragten
- die Aufsichtsbehörde
- die Haftung
- die Auftragsdatenverarbeitung
- das Verzeichnis der Verarbeitungstätigkeiten
- die Datenschutzfolgeabschätzung
- die Meldepflicht bei Datenpannen
- technisch-organisatorische Maßnahmen und
- die Datenübermittlung ins Ausland

werden in diesem Aufsatz ebenso vorgestellt.

Die DSGVO stellt einen nachhaltigen Wechsel im Datenschutz dar. Für die kommenden Jahre wird hier der Grundstock für das Vertrauen in den Datenschutz in Europa gelegt.

Worum geht es eigentlich beim Datenschutz im Unternehmen?

Beim Datenschutz im Unternehmen unterscheiden wir:

I. den internen Bereich:
Hier geht es um den datenschutzkonformen Umgang mit den personenbezogenen Daten der Beschäftigten.

II. den externen Bereich:
Hier geht es um den datenschutzkonformen Umgang mit den personenbezogenen Daten aller Personen, mit denen das

Unternehmen im Rahmen seiner Tätigkeit in Berührung kommt.

Zu beachten sind hier:

I. auf europäischer Ebene: EU Datenschutz-Grundverordnung (DSGVO) VO (EU) 679/2016
II. auf nationaler Ebene: Bundesdatenschutzgesetz (BDSG), u.a.

Grundrechtlich ist zu verweisen:

I. auf nationaler Ebene: Grundrecht auf informationelle Selbstbestimmung (siehe hierzu das Volkszählungsurteil des BVerfG vom 15.12.1983 *[BVerfGE 65,1]* sowie Art. 1 Abs. 1 GG *[Menschenwürde]* und Art. 2 Abs. 1 GG *[Persönlichkeitsrecht]*)
II. auf europäischer Ebene: Grundrecht auf den Schutz personenbezogener Daten (siehe hierzu Art. 8 Charta der Grundrechte der Europäischen Union *[EU-GRCharta]*

Die DSGVO gilt gemäß Art. 3 Abs. 1 für Verarbeiter und Auftragsverarbeiter in der EU als auch gemäß Art. 3 Abs. 2, so dass im Rahmen des Marktortprinzips die DSGVO auch für Anbieter aus den USA und anderen Drittstaaten gilt. Das Marktortprinzip ist dabei an folgende Bedingungen geknüpft:

1. Die Betroffenen sind in der EU ansässig.
2. Den Betroffenen werden Waren/Dienstleistungen angeboten oder die Verarbeitung dient zur Beobachtung des Verhaltens bzw. des/der Betroffenen.

In der Anwendung geht die DSGVO nationalen Datenschutzgesetzen stets vor. Mit Gesetz vom 30.6.2017 wurde das EU-Recht an das Bundesdatenschutzgesetz angepasst. Das „neue" Bundesdatenschutzgesetz tritt zum 25. Mai 2018 in Kraft.

Betrachten wir erst einmal die Legaldefintionen nach Art. 4 Nr. 1 DSGVO und Art. 9 Abs. 1 DSGVO.

Art. 4 Nr. 1 DSGVO:

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen:

Beispiel:

Name, Staatsangehörigkeit, vertragliche Beziehung zu Dritten, Beruf, Telefonnummer, E-Mail-Adresse, Beruf, Vermögen

Art. 9 Abs. 1 DSGVO:

Besondere personenbezogene Daten sind Angaben über: die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Daten zum Sexualleben oder Daten zur sexuellen Orientierung

Diese Daten werden in besonderem Umfang geschützt. Auch gelten gemäß Art. 9 Abs. 2 DSGVO strengere Maßstäbe für deren Handhabung.

Betriebs- und Geschäftsgeheimnisse unterliegen per se erst einmal nicht dem klassischen Datenschutz, sondern sind anderweitig geschützt. Hierunter fallen:

- vertraglich vereinbarte Geheimhaltungspflichten
- gesetzliche Geheimhaltungspflichten (z.B. § 30 AO, § 35 SGB I)
- standesrechtliche Geheimhaltungspflichten (Arztgeheimnis, Schweigepflicht der Rechtsanwälte)

Zu berücksichtigen sind hierbei auch die beiden Fallkonstellationen pseudonymisierte Daten (gemäß Art. 4 Nr. 5 DSGVO) und anonymisierte Daten gemäß ErwGr 26 Satz 5.

Bei pseudonymisierten Daten wird der Personenbezug dadurch erschwert, indem das Identitätsmerkmal durch ein Kennzeichnen ersetzt wird. Es handelt sich hier weiterhin um personenbezogene Daten mit der Folge, dass das Datenschutzrecht anwendbar bleibt.

Bei anonymisierten Daten handelt es sich um Daten, die einer Person nicht mehr zugeordnet werden können, zum Beispiel 12345678 statt Heinz Becker. Es handelt sich nicht mehr um personenbezogene Daten und das Datenschutzrecht ist auch nicht mehr anwendbar.

Was ist zulässige Verarbeitung im Sinne der DSGVO?

Gemäß Artikel 2 Nr. 2 DSGVO versteht man unter Verarbeitung jeden Vorgang oder jede Vorgangsreihe mit personenbezogenen Daten, die mit oder ohne Hilfe automatisierter Verfahren ausgeführt wird. Unterfälle des Verarbeitens sind das Erheben, das Speichern, das Übermitteln, die Einschränkung und das Löschen.

ERHEBEN ist das aktive Beschaffen von Daten über die betroffene Person (z.B. Befragung des Betroffenen oder Befragung bei Dritten). Der Zweck der Verarbeitung muss beim Erheben geklärt sein; Erheben löst Informationspflichten nach Art. 13 f. DSGVO aus.

Unter **SPEICHERN** versteht man das Erfassen, Aufnehmen, Aufbewahren personenbezogener Daten auf einem Datenträger zur weiteren Verarbeitung oder Nutzung, wobei auch Papier ein Datenträger sein kann. Die Aufbewahrungsdauer (Speicherdauer), die Zugriffsrechte müssen festgelegt sein und es muss gemäß Art. 15 DSGVO Auskunft über gespeicherte Daten gegeben werden.

ÜBERMITTELN ist das Bekanntgeben gespeicherter personenbezogener Daten an Dritte, wobei auch das Abrufen hierunter zu subsumieren ist. Die Übermittlung ist dabei an Zulässigkeitsvoraussetzungen geknüpft, wobei die Übermittlung in das Nicht-EU-Ausland besonders abzusichern ist.

Unter **EINSCHRÄNKEN** versteht man das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung / Nutzung einzuschränken.

LÖSCHEN ist das Unkenntlichmachen gespeicherter personenbezogener Daten. Wenn Dritte mit der Löschung beauftragt werden, so ist hierbei auch Art. 28 DSGVO (Auftragsverarbeitung) zu berücksichtigen. Des Weiteren wird in der Regel die DIN 66399 zu berücksichtigen sein.

Gemäß Artikel 6 DSGVO ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten verboten, es sei denn, dass eine Erlaubnis vorliegt.

Die Zulässigkeit der Verarbeitung nach Art. 6 Abs. 1 DSGVO kann gegeben sein durch:

- Einwilligung
- Vertrag oder vorvertragliche Maßnahmen
- Rechtliche Verpflichtung des Verantwortlichen
- Schutz lebenswichtiger Interessen
- Wahrnehmung einer Aufgabe im öffentlichen Interesse bzw. Ausübung öffentlicher Gewalt
- Überwiegende Interessen des Verantwortlichen

Die Struktur des neuen Bundesdatenschutzgesetzes

Das neue Bundesdatenschutzgesetz gliedert sich wie folgt:

Teil 1: Gemeinsame Bestimmungen §§ 1 bis 21
Teil 2: Durchführungsbestimmungen DSGVO, §§ 22 bis 44
Teil 3: Verarbeitungen gemäß JI-RL, RL (EU) 2016/680, §§ 45 bis 84
Teil 4: Besondere Bestimmungen § 85

Bevor wir uns die Details anschauen, sei zuerst einmal verwiesen, wo welche Anforderungen zu finden sind:

Zulässigkeit der Verarbeitung:
§ 3 BDSG n.F.

Videoüberwachung:
§ 4 BDSG n.F.

Verarbeitung besonderer personenbezoge-ner Daten:
§ 22 BDSG n.F.
Übermittlung
§ 25 BDSG n.F.
Beschäftigungsdaten
§ 26 BDSG n.F.
Technisch-organisatorische Maßnahmen
Art. 24,32 DSGVO
Datensparsamkeit/Datenverarbeitung
Art. 25 DSGVO
Auftragsverarbeitung
Art. 28 DSGVO
Verarbeitungsverzeichnis
Art. 30 DSGVO
Datenschutz-Folgeabschätzung (DSFA)
Art. 35 DSGVO
Datenschutzbeauftragte/r
Art. 37-39 DSGVO sowie §§ 5-7, 38 BDSG n.F.

Die/der Datenschutzbeauftragte/r

Ein Datenschutzbeauftragter ist gemäß Art. 37 Abs. 1 a-c DSGVO zu bestellen, wenn einer der nachfolgenden Voraussetzungen erfüllt ist:

- Behörde oder öffentliche Stelle (Ausnahme: Gerichte)
- Kerntätigkeit mit umfangreicher oder systematischer Überwachung von Personen
- Kerntätigkeit mit umfangreicher Verarbeitung besonders sensibler Daten im Sinne von Art. 9 f. DSGVO

Auf die nachfolgenden Aspekte ist im Sinne der DSGVO zu verweisen:

Art. 37 Abs. 2 DSGVO:
Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten benennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.

Art. 37 Abs. 6 DSGVO:
Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

Art 37 Abs. 7 DSGVO:
Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

Wie ein Vergleich mit Art. 13 Abs. 1 a DSGVO zeigt – wo von Name und Kontaktdaten die Rede ist – setzt die Angabe der bloßen Kontaktdaten, z.B. auf der Homepage nicht voraus, dass auch der Name des Datenschutzbeauftragten genannt wird. Gemäß Art. 30 Abs.1 a in Verbindung mit Art. 4 DSGVO ist die namentliche Nennung des Beauftragten im Verhältnis zur Aufsichtsbehörde jedoch sinnvoll.

Die Bundesrepublik Deutschland hat in Sachen Datenschutzbeauftragter von der DSGVO Öffnungsklausel Gebrauch gemacht und durch § 38 BDSG n.F. eine Pflicht zur Bestellung eines Datenschutzbeauftragten festgelegt, wenn:

1. mindestens zehn Personen ständig mit automatisierter Verarbeitung befasst sind oder
2. der Verantwortliche Verarbeitungen vornimmt, die der Datenschutzfolgeabschätzung nach Art. 35 DSGVO unterliegen oder
3. der Verantwortliche Daten gewerbsmäßig zum Zweck der Übermittlung, Markt- und Meinungsforschung verarbeitet.

§ 38 Abs.2 BDSG verweist dabei auf wichtige Grundregeln:

- Abberufungsschutz, § 6 Abs. 4 BDSG n.F.
- Verschwiegenheitspflicht § 6 Abs. 5 Satz 2 BDSG n.F.
- Zeugnisverweigerungsrecht, § 6 Abs. 6 BDSG n.F.

Der Datenschutzbeauftragte muss ein Fachwissen mitbringen und persönlich geeignet sein. Nach Art. 37 Abs. 5 DSGVO muss ein Fachwissen auf dem Gebiet des Datenschutzrechtes und der Datenschutzpraxis ebenso vorhanden sein wie die Fähigkeit zur Erfüllung der in Art. 39 DSGVO genannten Aufgaben. Dies Trias aus rechtlichen, technischen und organisatorischen Kenntnissen ist jedoch nicht mehr zwingend nachzuweisen.

Die Mindestaufgaben des Datenschutzbeauftragten sind durch Artikel 39 Abs. 1 DSGVO wie folgt definiert:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung und den sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedsstaaten
- Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedsstaaten sowie der Strategien der Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten inkl. der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen
- Auf Anfrage Beratung im Zusammenhang mit der Datenschutzfolgeabschätzung und Überwachung Ihrer Durchführung gemäß Artikel 35 DSGVO
- Zusammenarbeit mit der Aufsichtsbehörde
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, inklusive der vorherigen Konsultation gemäß Artikel 36 DSGVO sowie gegebenenfalls Beratung zu allen sonstigen Fragen

Gemäß Artikel 39 Abs. 2 DSGVO hat der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiken Rechnung zu tragen. Art, Umfang, Umstände sowie die Zwecke der Verarbeitung sind im Rahmen der Pflicht zur risikoorientierten Tätigkeit zu berücksichtigen.

Auf die Strafbarkeit gemäß § 203 Abs. 4 StGB für Datenschutzbeauftragte wird explizit verwiesen.

Für die Zusammenarbeit zwischen Datenschutzbeauftragten und Betriebsrat gibt es keinerlei gesetzliche Regelungen. So hat der Betriebsrat zum Beispiel auch kein Mitspracherecht bei der Bestellung. Der Betriebsrat ist selbst auch zur Einhaltung des Datenschutzes der ihm anvertrauten Daten verpflichtet. In diesem Zusammenhang wird auf die Grundsatzentscheidung des Bundesarbeitsgerichtes BAG verwiesen, wonach dieser ein Kontrollrecht des Datenschutzbeauftragten bei Datenverarbeitung durch den Betriebs-/Personalrat ablehnt (NJW 1998, S. 2466). Nach § 75 Abs. 3 Nr. 17 BPersVG, § 87 Abs. 1 Nr. 6 BetrVG hat der Betriebs-/Personalrat ein Mitbestimmungsrecht bei der Einführung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder Leistung der Beschäftigten zu überwachen (z.B. Zeiterfassung, Protokolldaten, Telefondatenerfassung). In Sachen Personalbögen hat der Betriebs-/Personalrat (§ 94 BetrVG, § 75 Abs.3 Nr. 8 BPersVG) nur bei der Erhebung ein Mitbestimmungsrecht, für die Speicherung und Verarbeitung existieren nämlich bereits gesetzliche Grundlagen. Bezüglich der Durchführung von Schulungen wird in diesem Zusammenhang auf § 96 BetrVG sowie § 75 Abs. 3 Nr. 7, § 76 Abs. 2 Nr. 6 BPersVG verwiesen. Eine Betriebsvereinbarung zum Datenschutz mag wünschenswert sein, gleichwohl ist diese nicht verpflichtend.

Die Aufsichtsbehörde

Alleine in den Artikel 51 bis 76 der DSGVO finden sich 26 Vorschriften zu den Aufsichtsbehörden. Als wichtigste Bereiche sind zu nennen:

- Aufgaben und Befugnisse, Art. 57 f. DSGVO
- Zusammenarbeit, Art. 60-62 DSGVO
- Kohärenzverfahren, Art. 63-67 DSGVO
- Europäischer Datenschutzausschuss, Art. 68ff. DSGVO
- Sanktionen, Art. 83 DSGVO

Als Aufgaben sind gemäß Art. 57ff. DSGVO zu nennen:

- Kontrolle
- Beratung
- Bearbeitung von Eingaben von Bürgern
- Information der Bürger

Befugnisse der Aufsichtsbehörde sind:

- Abberufungsrecht: Der Datenschutzbeauftragte kann von der Aufsichtsbehörde in begründeten Fällen abberufen werden.
- Auskunft zu Fragen sowie in Einsicht in alle Unterlagen, vor allem in die gespeicherten Daten und in die Datenverarbeitungsprogramme
- Jederzeit Zutritt zu allen Räumen

Kontrollarten sind:

- anlassbezogene Kontrollen, z.B.: im Rahmen der Eingabe von Bürgern
- themenbezogene Kontrollen, z.B. Prüfung / Lösung grundsätzlicher Probleme
- Querschnittskontrolle, z.B. zum Kennenlernen einer Branche

Die Aufsichtsbehörde kann bei Verstößen gegen den Datenschutz Geldbußen verhängen, wobei Verstöße gegen die DSGVO „wehtun“ sollen. Gemäß Art. 79 Abs. 3a DSGVO können die Geldbußen bis zu 20 Millionen Euro betragen. Berechnungsgrundlage ist dabei der Umsatz des Vorjahres (4 Prozent Regel).

Gemäß § 40 Abs. 1 BDSG n.F. überwachen die nach Landesrecht zuständigen Behörden die nichtöffentlichen Stellen. Dies sind in der Regel die Landesdatenschutzbeauftragten.

Betroffenenrechte

Als Betroffenenrechte sind gemäß des BDSG n.F. zu nennen:

- § 32: Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
- § 33: Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
- § 34: Auskunftsrecht der betroffenen Person
- § 35: Recht auf Löschung
- § 36: Widerspruchsrecht
- § 37: Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

Gemäß Art. 15 DSGVO/§ 34 BDSG besteht ein Recht auf Auskunft, ob der Verantwortliche personenbezogene Daten verarbeitet hat oder nicht. Das Recht umfasst folgende Informationen:

- Verarbeitungszwecke
- Kategorien von Daten
- Empfänger der Daten
- Dauer der Speicherung oder Kriterien zu deren Festlegung
- Bestehen eines Berichtigungs-, Löschungs-, Widerspruchs-, Beschwerderechts
- Herkunft der Daten

Auskunftserteilungen müssen nach Art. 12 Abs. 3 DSGVO unverzüglich, spätestens aber innerhalb eines Monates erfolgen. Nur in begründeten Ausnahmefällen -über die die betroffene Person aber zu informieren istdarf die Monatsfrist überschritten werden. Nach Art. 12 Abs. 5 S. 3 DSGVO muss die Auskunftserteilung für die Erstauskunft kostenfrei erfolgen, wobei für weitere Kopien ein „angemessenes“ Entgelt verlangt werden kann.

Im Rahmen von Art. 16 DSGVO haben Betroffene ein Recht auf Berichtigung oder Vervollständigung der Daten.

Das Recht auf Vergessenwerden/Löschen ist durch Art. 17 DSGVO/§ 35 BDSG n.F. normiert. Ein Verarbeiter muss personenbezogene Daten löschen, wenn:

1. sie für den Erhebungszweck nicht mehr erforderlich sind, oder
2. die Einwilligung zur Verarbeitung widerrufen wird, oder
3. die Verarbeitung unrechtmäßig ist

Ein Folgenbeseitigungsanspruch besteht, wenn die Daten durch den Verantwortlichen veröffentlicht wurden. Bei der Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt ist das Recht auf Löschung nicht gegeben.

Haftungsfragen nach dem neuen Datenschutzrecht

Nach Art. 82 DSGVO haften Unternehmer und Auftraggeber für materiellen und immateriellen Schaden, welcher aufgrund eines Verstoßes gegen die DSGVO entstanden ist. Ein Auftragsverarbeiter haftet (auch), wenn er die Weisung des Auftraggebers nicht beachtet. Eine Haftung entfällt in der Regel nur dann, wenn der für die Verarbeitung Verantwortliche nachweisen kann, dass er nicht für den Schaden verantwortlich ist. Im Rahmen der Haftung ist im Übrigen eine gesamt-schuldnerische Haftung gegeben.

Gemäß § 831 BGB (Haftung aus Deliktrecht) haftet ein Unternehmen für Handlungen seiner Mitarbeiter, die es als Verrichtungsgehilfen ausgewählt hat, es sei denn es liegt eine Exkulpierung dergestalt vor, dass der Mitarbeiter sorgfältig ausgewählt und überwacht wurde. Die Exkulpationsmöglichkeit greift jedoch nicht bei Organen eines Unternehmens (§§ 30 f. BGB).

Eine Haftung aus Deliktrecht (§ 823 BGB) ist gegeben, wenn ein Eingriff in das Persönlichkeitsrecht des Betroffenen vorliegt. Obgleich sich der Anspruch gegen den Mitarbeiter wendet, der die Handlung begangen hat, hat der Mitarbeiter in der Regel aber nach den Grundsätzen des innerbetrieblichen Schadensausgleiches einen Anspruch auf vollständige oder teilweise Freistellung durch das Unternehmen.

In Artikel 83 DSGVO finden sich die Datenschutzverstöße, welche zu einer Geldbuße führen können, die von der Aufsichtsbehörde gemäß Art. 41 BDSG festgesetzt werden.

Die Strafvorschrift ist durch § 42 BDSG gegeben. Hiernach wird mit einer Freiheitsstrafe bis zu 2 Jahren oder Geldstrafe bestraft, wer allgemein nicht zugängliche Daten ohne Berechtigung verarbeitet oder unter falschen Angaben erschleicht und dies gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht tut. Die Tat wird jedoch nur auf Antrag von Betroffenen, Verantwortlichen oder der Aufsichtsbehörde verfolgt.

Auch der Datenschutzbeauftragte kann strafrechtlich belangt werden, wen er für einen Bereich zuständig ist, in dem gemäß § 203 StGB Verschwiegenheitspflichten gelten und er gleichwohl unbefugt Daten übermittelt, verarbeitet oder erschleicht. Neben § 203 StGB ist hier auch der § 42 BDSG in Betracht zu ziehen.

Auftragsdatenverarbeitung

Nach Art. 4 Nr. 8 DSGVO ist Auftragsverarbeiter eine Stelle, welche personenbezogene Daten im Auftrag des

Verantwortlichen verarbeitet. Verantwortlicher nach Art. 4 Nr. 7 DSGVO ist die Stelle, die allein oder gemeinsam mit Dritten über die Mittel und die Zwecke der Verarbeitung personenbezogener Daten entscheidet.

Für die Weitergabe personenbezogener Daten an den Auftragsverarbeiter und die Verarbeitung durch den Auftragsverarbeiter bedarf es in der Regel keiner weiteren Rechtsgrundlage gemäß Art. 6 bis 10 DSGVO. Gleichwohl muss wie bisher zwischen den beiden Vertragsparteien ein schriftlicher oder in einem elektronischen Format abgefasster Vertrag vorliegen, wobei die Gesamtverantwortung für die Datenverarbeitung und die Nachweispflicht gemäß Art. 5 Abs. 2 DSGVO nach wie vor beim Verantwortlichen verbleibt. Nur wenn der Auftragsverarbeiter die zu verarbeitenden Daten vertragswidrig verarbeitet, gilt er nach Art. 28 Abs. DSGVO selbst als Verantwortlicher und muss dann alle rechtlichen Folgen tragen. Nach der neuen DSGVO muss der Auftragsverarbeiter selbst ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO führen. Verstoßen Auftragsverarbeiter gegen datenschutzrechtliche Bestimmungen, so können gemäß Art. 28 DSGVO Geldbußen von bis zu 10.000.000 Euro oder bis zu 2 % des gesamten weltweiten Jahresumsatzes des vergangenen Jahres von der Aufsichtsbehörde verhängt werden.

Gemäß Anhang A Art. 28 DSGVO liegt eine Auftragsverarbeitung auch in folgenden Fällen vor:

- DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren
- Auslagerung der Backup-Sicherheitsspeicherung und anderer Archivierungen
- Datenträgerentsorgung durch Dienstleister
- Fernwartung, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann
- Zentralisierung bestimmter Shared Service Dienstleistungen
- Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud Computing

Keine Auftragsverarbeitung liegt gemäß Anhang B Art. 28 DSGVO bei Berufsgeheimnisträgern wie Steuerberater, Rechtsanwälte, externe Betriebsärzte oder Wirtschaftsprüfern vor.

Verzeichnis der Verarbeitungstätigkeiten

Organisation mir weniger als 250 Mitarbeitenden müssen gemäß Art. 30 Abs. 5 DSGVO kein Verzeichnis von Verarbeitungstätigkeiten führen. Diese Begrenzung gilt jedoch dann nicht, wenn eine Verarbeitung personenbezogener Daten durchgeführt wird,

- welche Risiken für die Rechten und Pflichten der betroffenen Personen birgt oder
- die nicht nur gelegentlich erfolgt oder
- die besondere Datenkategorien gemäß Art. 9 Abs. 1 DSGVO oder strafrechtliche Verurteilungen/ Straftaten nach Art. 19 DSGVO betreffen

Nach dem neuen Datenschutzrecht ist weder ein öffentliches Verzeichnis noch eine Meldepflicht mehr gegeben, wie dies früher war.

Während die Vorgaben für Verzeichnisse für Verantwortliche durch Art. 30 Abs. 1 DSGVO bestimmt sind, sind die Anforderungen für den Inhalt eines Verzeichnisses für Auftragsverarbeiter durch Art. 30 Abs. 2 DSGVO definiert.

Sowohl für Verarbeiter als auch für Auftragsverarbeiter müssen in den Verzeichnissen allgemeine Beschreibungen der technischen und organisatorischen Maßnahmen zu finden sein, wobei nicht definiert ist, wie detailliert die Beschreibung sein muss. Hierzu wird auf Art. 32 DSGVO verwiesen.

Neben den Verzeichnissen der Verarbeitungstätigkeiten gibt es noch weitere Dokumentationspflichten, welche zu berücksichtigen sind, so zum Beispiel:

- das Vorhandensein von Einwilligen (nach Art. 7 Abs. 1 DSGVO)
- die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1 DSGVO)
- das Ergebnis von Datenschutzfolgeabschätzungen (Art. 35 Abs. 7 DSGVO)

Datenschutzfolgenabschätzung

Die Datenschutzfolgeabschätzung (DSFA) nach Art. 35 DSGVO ist ein Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Im Rahmen der DSFA muss der Verantwortliche Verarbeitungen mit hohem Risiko überprüfen, bevor sie beginnen. Hierdurch soll sichergestellt sein, dass angemessene Schutzmaßnahmen vor dem hohen Risiko vorgesehen sind.

Neben den in Art. 35 Abs. 3 DSGVO genannten Gründen muss eine DSFA in den folgenden Fällen durchgeführt werden:

1. nach ErwGr 91, wenn Verfahren eingesetzt werden,
   - die nach Auffassung der zuständigen Aufsichtsbehörde wahrscheinlich ein hohes Risiko für Freiheiten und Rechte der betroffenen Personen mit sich bringen
   - bei denen den Betroffenen die Ausübung ihrer Rechte erschwert wird
2. nach Leitfaden WP 248 der Art. 29 – Gruppe in den folgenden Fällen:
   - Bewertung und Scoring inkl. Prognosen und Profilerstellung
   - automatisch erfolgende Entscheidungen mit rechtlichen oder vergleichbaren Auswirkungen für Dritte
   - systematisches Monitoring
   - sensitive, vor allem personenbezogene Daten
   - umfangreiche Datenmengen
   - Vergleich oder Kombination von Datensätzen
   - Daten ungeschützter Betroffener
   - Einsatz innovativer Technologien oder neuartiger organisatorischer Lösungen
   - Datentransfers in Länder außerhalb der EU/EWR
   - Verhinderung, dass die betroffene Person ein Recht ausüben kann

Die Aufsichtsbehörden sind gemäß Art. 35 Abs. 4 DSGVO verpflichtet, eine Positiv-Liste für diejenigen Verfahren zu erstellen, bei denen auf jeden Fall eine DSFA durchzuführen ist. Sie kann eine Negativ-Liste für Verarbeitungen erstellen, für die keine DSFA durchzuführen ist.

Der Mindestinhalt der Prüfung ist durch Art. 35 Abs. 7 DSGVO normiert:

1. Systematische Beschreibung der geplanten Verarbeitungen und der zugehörigen Verarbeitungszwecke
2. Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge
3. Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
4. Bewertung der zur Bewältigung der Risiken geplanten Abhilfemaßnahmen

Kommt die DSFA zu dem Ergebnis, dass die Verarbeitung unzulässig ist, kann der Verantwortliche sich zur „vorherigen Konsultation“ nach Art.

36 an die für ihn zuständige Landesbehörde wenden.

Diese prüft, berät und entscheidet innerhalb von 8 Wochen über die Zulässigkeit. Die Datenschutzfolgeabschätzung wird vom Verantwortlichen durchgeführt, d.h. die Leitung muss die Aufgabe einer Stelle zur Erledigung zuweisen. Gemäß Art. 39 Abs. 1 c) DSGVO hat der Datenschutzbeauftragte hierbei „nur" Beratungsfunktion.

Meldepflicht bei Datenpannen

Als Datenpanne im Sinne von Art. 33 f. DSGVO erachtet man die Verletzung des Schutzes personenbezogener Daten

- aufgrund Vernichtung oder Veränderung
- aufgrund Zugang oder Offenlegung
- oder in sonstiger Weise

Bei Datenpannen ist eine Risikoeinschätzung vorzunehmen, ob ein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Es besteht in der Regel gegenüber der Aufsichtsbehörde und den Betroffenen eine zeitlich definierte Informationspflicht.

Technisch-organisatorische Maßnahmen

Aus dem Prinzip der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 DSGVO werden die technisch-organisatorischen Maßnahmen (TOM) abgeleitet die bewirken (sollen), dass das Ziel des Datenschutzes erreicht wird.

Die TOM müssen im Rahmen einer Dokumentation nachgewiesen als auch überprüft und aktualisiert werden. Gemäß Artikel 25 DSGVO müssen die Datenschutzgründe bereits bei der Festlegung berücksichtigt werden und es müssen restriktive Voreinstellungen bzgl. des Umfangs, der Zugriffsrechte und Speicherdauer der personenbezogenen Daten vorliegen.

In Art. 32 Abs. 1 a) bis d) DSGVO werden exemplarisch nachfolgende Maßnahmen aufgeführt:

- Pseudonymisierung und Verschlüsselung
- Vertraulichkeit, Integrität, Verfüg-barkeit und Belastbarkeit der Verarbeitungssysteme
- Wiederherstellung der Verfügbarkeit und des Zuganges nach einem Zwischenfall
- Verfahren zur regelmäßigen Evaluierung der getroffen TOM

Telekommunikationsgeheimnis

Der Schutzbereich des Fernmeldegeheimnisses ist der Schutz der unkörperlichen Übermittlung individueller Kommunikation, unabhängig von der Übertragungstechnik und unabhängig vom Inhalt.

Während für staatliche Stellen in der Regel Art. 10 GG die Normierungsgrundlage ist, ist die Anspruchsgrundlage für Dienstanbieter im nicht-öffentlichen Bereich § 88 TKG. Diesbezüglicher Dienstanbieter ist jeder, der ganz oder teilweise geschäftsmäßig TK-Dienste erbringt oder bei der Erbringung solcher mitwirkt, § 3 Nr. 6 TKG. Dadurch, dass ein Unternehmen die private Nutzung von Telekommunikationsdiensten zulässt, wird es zum Diensteanbieter im Sinne des Telekommunikationsgesetzes (TKG).

Hiernach geschützt sind:

1. Inhalt der Telekommunikation
2. Nähere Umstände der Telekommunikation
3. Beteiligte am Telekommunikationsvorgang
4. Erfolglose Verbindungsversuche und damit zusammenhängende Verkehrsdaten

In der Regel verboten ist die Kenntnisnahme des Inhaltes oder der näheren Umstände der Kommunikation. In § 96 TKG ist geregelt, welche Verkehrsdaten erhoben werden dürfen.

Neben dem TKG sind in diesem Zusammenhang auch zu beachten:

- § 206 StGB:
  Verletzung des Post- oder Fernmeldegeheimnisses
- § 201 StGB:
  Verletzung der Vertraulichkeit des Wortes

Datenübermittlung ins Ausland

Die Datenschutzgrundverordnung befasst sich in den Artikeln 44 bis 49 mit der Datenübermittlung an Länder außerhalb der EU/des EWR. Diese Länder werden als so genannte „Drittstaaten" bezeichnet.

Es erfolgt hier eine Zwei-Stufen-Prüfung.

Stufe 1:
Halten die Drittländer neben den in Art. 45 ff. DSGVO spezifischen Anforderungen alle übrigen Anforderungen der DSGVO (z.B. auch Art. 9 Abs. 3 DSGVO) ein?

Stufe 2:
Werden die in Artikel 45 ff. genannten Anforderungen erfüllt?

Für nichtöffentliche Stellen gibt es folgende Möglichkeiten des Datentransfers in Drittländer:

- Feststellung der Angemessenheit des Datenschutzniveaus im Drittland durch die EU-Kommission (Art. 45 DSGVO)
- Vorliegen geeigneter Garantien (Art. 46 DSGVO)
- Ausnahmen für bestimmte Fälle (Art. 49 DSGVO)

Fazit

Der vorstehende Aufsatz mag hoffentlich aufgezeigt haben, dass die DSVGO mehr als nur eine redaktionelle Anpassung war und dass hier ein Paradigmenwechsel stattgefunden hat.

Hinweis

Ausdrücklich wird in diesem Zusammenhang darauf verwiesen, dass dieser wissenschaftliche Artikel keine Beratung in Rechtsfragen ersetzen kann und auch nicht als Rechtsberatung angedacht ist. Dieser Fachartikel kann auch keine unternehmensspezifischen Fragen beantworten, sondern liefert nur allgemeine Aussagen zu den Neuerungen des Datenschutzes durch die EU Datenschutzgrundverordnung und die Umsetzung durch das ab dem 25.5.2018 gültige (neue) Bundesdatenschutzgesetz.

Author Prof. h.c.(IUK) PhDr. Dipl.-Kfm./ Dipl.-Vw. Stefan Loubichi
Loubichi Business Consulting UG (haftungsbeschränkt)
Associate expert to Kraftwerksschule Essen and Simulator Centre Essen (GfS mbH / KSG mbH)
Grafenberger Allee 125
40237 Düsseldorf