Leseprobe aus
Computer und Recht 08/2017
Dr. Otto Schmidt Verlag

CR Daten und Sicherheit

Michael Rath/Gerrit Feuerherdt

Datenschutz-Folgenabschätzung als Standard im Konzern: Hinweise zur Anwendung des Kriteriums „hohes Risiko" einer Datenverarbeitung und Vorschläge zur Verknüpfung mit dem Standard-Datenschutzmodell sowie den ISO-Standards 29100 und 29134

Mit der am 25.5.2018 in Kraft tretenden EU-Datenschutz-Grundverordnung (DSGVO) wird u.a. die Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO neu eingeführt. Die Artikel-29-Datenschutzgruppe hat in ihrem Arbeitspapier vom 4.4.2017 Richtlinien für die Durchführung einer solchen Datenschutz-Folgenabschätzung erlassen und darin Vorschläge gemacht, wann diese obligatorisch sein soll. Dieser Beitrag setzt sich mit den Kriterien einer Datenschutz-Folgenabschätzung auseinander und verknüpft die Datenschutz-Folgenabschätzung mit anderen datenschutzrechtlichen Modellen, namentlich dem Standard-Datenschutzmodell der deutschen Datenschutzaufsichtsbehörden und den internationalen Standards ISO/IEC 29100:2011 und ISO 29134:2017.

I. Risikobasierte Folgenabschätzung und Bestrebungen zur Standardisierung

In Deutschland existieren bereits mit Folgenabschätzungen in anderen Bereichen (Technik, Umwelt, Gesetzgebung etc.) mit der Datenschutz-Folgenabschätzung vergleichbare Prozesse[1]. Die Datenschutz-Folgenabschätzung nach Art. 35 DGSVO ersetzt nunmehr faktisch in Deutschland das Institut der Vorabkontrolle im Datenschutz nach § 4d Abs. 5 BDSG[2].

1. Bisherige Erfahrungen mit Datenschutz-Folgenabschätzungen

International ist das Prinzip einer Datenschutz-Folgenabschätzung hingegen schon länger bekannt: In Großbritannien gibt es mit dem Handbuch der britischen Datenschutzbehörde (Information Commissioner's Office, kurz ICO) seit 2014[3] bzw. in Frankreich durch verschiedene Veröffentlichungen der dortigen Behörde für Datenschutz und Informationsfreiheit (Commission Nationale de l'Informatique et des Libertés, kurz CNIL) seit 2015 Richtlinien zur Durchführung einer Datenschutz-Folgenabschätzung[4]. Außerhalb der EU ist das Instrument der Datenschutz-Folgenabschätzung vornehmlich im angelsächsischen Raum bekannt, wenn auch oft uneinheitlich und unverbindlich geregelt[5]. Die deutschen Datenschutzaufsichtsbehörden haben sich nach dem Inkrafttreten der DSGVO intensiver mit der Datenschutz-Folgenabschätzung beschäftigt. Neben verschiedenen Stellungnahmen der Behörden[6] existiert seit November

▷ RA und FA für IT-Recht Dr. Michael Rath ist Partner, Gerrit Feuerherdt ist wissenschaftlicher Mitarbeiter im Kölner Büro der Luther Rechtsanwaltsgesellschaft mbH.

1 *Martini* in Paal/Pauly, Datenschutz-Grundverordnung, 1. Aufl. 2017, DS-GVO Art. 35 Rz. 2 f., Rz. 74 ff.; *Schmitz/von Dall'Armi*, ZD 2017, 57; www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf, S. 7 ff.

2 *Hamann*, BB 2017, 1090 (1094).

3 https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

4 https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf; https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf.

5 www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf, S. 9 f., m.w.N.

6 Siehe z.B. die Stellungnahme des *Landesbeauftragten für den Daten-*

Leseprobe aus Computer und Recht 08/2017 - Dr. Otto Schmidt Verlag

2016 mit dem „Standard-Datenschutzmodell“[7] eine Grundlage, die sowohl Behörden als auch Unternehmen bei der Umsetzung der DSGVO etwas „an die Hand geben soll“. Hierauf kann auch für Datenschutz-Folgenabschätzungen zurückgegriffen werden[8].

2. Internationale Standards

Mit den Normen der ISO (International Organization for Standardization) und der IEC (International Electrotechnical Commission) im Datenschutz und bei Datenschutz-Folgenabschätzungen existieren mittlerweile auf internationaler Ebene Leitlinien zur Vereinheitlichung der Vorgehensweise. Die ISO/IEC-Norm 29100:2011 stellt (vergleichbar mit dem deutschen Standard-Datenschutzmodell) Prinzipien auf, die im Datenschutz allgemein gelten und bei jeder Datenverarbeitung zu beachten sein sollen[9]. Die ISO/IEC 29134:2017 beschreibt detailliert den Ablauf einer Datenschutz-Folgenabschätzung von der Vorbereitungs- über die Durchführungs- bis hin zur Nachbereitungs- und Reportphase[10].

3. Datenschutz-Folgenabschätzung nach der DSGVO

Eine Datenschutz-Folgenabschätzung ist nach Art. 35 DSGVO immer dann erforderlich, wenn durch die jeweilige Datenverarbeitung voraussichtlich hohe Risiken für die Rechte und Freiheiten natürlicher Personen drohen. In Art. 35 Abs. 3 DSGVO werden drei Kategorien an Datenverarbeitung genannt, in denen eine Datenschutz-Folgenabschätzung zwingend durchzuführen ist, weil sie vom Gesetzgeber stets als risikobehaftet angesehen werden[11]. Die Aufzählung ist jedoch nicht abschließend; vielmehr ist gem. Art. 35 Abs. 1 DSGVO auch in anderen Fällen, in denen voraussichtlich hohe Risiken durch eine Datenverarbeitung drohen, eine Datenschutz-Folgenabschätzung durch den Verantwortlichen durchzuführen, um Risiken im Bereich des Datenschutzes erfassen und gegebenenfalls entgegensteuern zu können[12].

II. Das „Ob“: Wann ist eine Datenschutz-Folgenabschätzung Pflicht?

Das Kriterium „hohes Risiko“ wird in der DSGVO nicht explizit definiert, so dass, trotz der Erläuterungen des Gesetzgebers in den Erwägungsgründen Nr. 75 bis 77, 89 und 91 zur DSGVO, Unklarheiten bei der genauen Bestimmung dieses Kriteriums verbleiben. Deshalb hat die *Artikel-29-Datenschutzgruppe*[13] Leitlinien und Kriterien vorgeschlagen, wann ein hohes Risiko gegeben und wann eine Datenschutz-Folgenabschätzung erforderlich sein soll[14].

1. Leitlinie der Artikel-29-Datenschutzgruppe

Die *Artikel-29-Datenschutzgruppe* orientiert sich bei ihrer Leitlinie u.a. an den Erwägungsgründen der DSGVO zur Datenschutz-Folgenabschätzung. Sie greift die Erwägungsgründe auf und erläutert sie anhand von Beispielen. So soll z.B. ein erheblicher Umfang gegeben sein, wenn die Datenverarbeitung eine hohe absolute oder relative Zahl der Bevölkerung betreffe oder das Datenvolumen oder die Datensätze einen großen Umfang annehmen. Auch die Dauer oder der geographische Umfang der Datenverarbeitung sollen mit einbezogen werden bei der Bewertung des Umfangs. Darüber hinaus schlägt die *Artikel-29-Datenschutzgruppe* als Daumenregel vor, dass bei einer Datenverarbeitung, die mindestens zwei der vorgenannten Kriterien erfüllt, grundsätzlich eine Datenschutz-Folgenabschätzung erforderlich ist. Denn erst dann sei ein „hohes Risiko“ i.S.d. Art. 35 Abs. 1 DSGVO anzunehmen. Sie weist aber zugleich auch darauf hin, dass in Ausnahmefällen schon das Vorliegen nur eines Kriteriums zur Notwendigkeit einer Datenschutz-Folgenabschätzung führen kann. Dies führe im Ergebnis dazu, dass bei Zweifeln an der Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung eine solche stets erfolgen sollte[15].

2. Beurteilung

Dieser Ansicht kann sich nur angeschlossen werden. Denn für die Vorgehensweise vor und während einer Datenschutz-Folgenabschätzung gibt die DSGVO keine expliziten Anweisungen an die Hand. In Art. 35 Abs. 7 DSVO werden lediglich inhaltliche Mindestanforderungen beschrieben[16]. Im Hinblick auf die daraus resultierende Unsicherheit sowohl auf Seiten der Verantwortlichen als auch der Aufsichtsbehörden sollte eine Datenschutz-Folgenabschätzung im Zweifel zur Absicherung immer durchgeführt werden. Dies gilt insbesondere, da auch die Nichtdurchführung einer Datenschutz-Folgenabschätzung gem. Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO ausführlich begründet werden muss. Denn es gehört im Rahmen der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO zu den Pflichten der datenverarbeitenden Stelle nachzuweisen, dass die technisch-organisatorischen Anforderungen und Datenschutzgrundsätze aus Art. 5 Abs. 1 DSGVO eingehalten werden. Darüber hinaus muss gem. Art. 24 Abs. DSGVO eine verordnungskonforme Datenverarbeitung durch entsprechende technisch-organisatorische Maßnahmen sichergestellt und nachgewiesen werden. Eine Datenschutz-Folgenabschätzung ist mithin ein zentrales Mittel zur Evaluation von Risiken für die betroffene Personen und damit u.a. ein Ausfluss der Grundsätze „Integrität“ und „Vertraulichkeit“ (Art. 5 Abs. 1, lit. f DSGVO), so dass eine Nichtdurchführung begründet und dokumentiert werden muss, um Aufsichtsbehörden gegenüber darlegen zu können, dass trotzdem die Grundsätze der DSGVO beachtet wurden[17].

schutz und die Informationsfreiheit Rheinland-Pfalz, https://www.datenschutz.rlp.de/de/themenfelder-themen/datenschutz-grundverordung/datenschutzfolgeabschaetzung/; oder des *Bayerischen Landesamtes für Datenschutzaufsicht*, https://www.lda.bayern.de/media/baylda_ds-gvo_18_privacy_impact_assessment.pdf.

7 https://www.datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf, S. 5 ff.

8 https://www.datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf, S. 6, 27.

9 ISO/IEC 29100:2011, S. VI, S. 1, 14–19.

10 ISO/IEC 29134:2017, S. 6 ff.

11 *Martini* in Paal/Pauly, Datenschutz-Grundverordnung, 1. Aufl. 2017, DS-GVO Art. 35, Rz. 28.

12 Erwägungsgründe Nr. 75–77, 84, 89 ff. DSGVO.

13 Die Datenschutzgruppe hat nach Art. 30 der RL 95/46/EG vornehmlich beratende Funktion gegenüber der europäischen Kommission bei Fragen des Datenschutzes. Sie kann selbstständig Empfehlungen und Stellungnahmen abgeben, allerdings sind diese nicht bindend für die europäische Kommission.

14 WP29 Guidelines on Data Protection Assessment, Working Paper No. 248.

15 WP29 Guidelines on Data Protection Assessment, Working Paper No. 248, S. 7–10.

16 *Martini* in Paal/Pauly, Datenschutz-Grundverordnung, 1. Aufl. 2017, DS-GVO Art. 35, Rz. 44.

17 *Hamann*, BB 2017, 1090 (1091), geht sogar so weit, dies als Beweislastumkehr einzuordnen.