Dossier III - Meldepflichten und Sanktionen

November 2018

Prof. Dr. Anne Riechert

Rechtsgrundlage:

Artikel 33, 34 Datenschutzgrundverordnung und Erwägungsgründe 85 bis 88 (Meldung und Benachrichtigung von Datenschutzverstößen)

Artikel 83 Datenschutzgrundverordnung und Erwägungsgründe 148 bis 152 (Allgemeine Bedingungen für die Verhängung von Geldbußen)

Dieses Dossier befasst sich mit Meldepflichten bei Datenschutzverstößen gegenüber Aufsichtsbehörden (A.), ebenso unter Beachtung der Sanktionsmöglichkeiten (B.). Unter Punkt C. folgt eine Zusammenfassung. Eine Sammlung mit weiterführenden Links findet sich am Ende der Ausführungen (D.).

A. Datenpannen und Meldepflichten

Nach altem Recht (BDSG) galt eine Meldepflicht bei Datenschutzverstößen nur bei einer unrechtmäßigen Übermittlung von sensiblen Daten (auch Kontodaten) an Dritte, wobei zusätzlich eine schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen musste.

Nach der Datenschutzgrundverordnung (Artikel 33 DSGVO) besteht immer eine unverzügliche Meldepflicht (binnen höchstens 72 Stunden) an die zuständige Aufsichtsbehörde, es sei denn der Verantwortliche kann nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Ob ein solches Risiko vorliegt, kann zu Untersicherheiten bei den Unternehmen führen. Als Hilfestellung hat die Datenschutzkonferenz ein entsprechendes Kurzpapier zur Einschätzung eines Risikos für die Rechte und Freiheiten natürlicher Personen veröffentlicht (https://www.lda.bayern.de/media/dsk_kpnr_18_risiko.pdf).

In der Praxis wird teilweise die Auffassung vertreten, dass es ausschließlich auf den Sitz des datenverarbeitenden Unternehmens ankommt und der Wohnsitz der betroffenen Person unerheblich ist, so dass es für Unternehmen mit Sitz außerhalb der EU keine zuständige Aufsichtsbehörde gibt, welcher innerhalb von 72 Stunden die Datenschutzverletzung zu melden ist. Dies würde jedoch den angestrebten Schutzzweck der Datenschutzgrundverordnung in sein Gegenteil verkehren. Sofern ein Unternehmen keine Niederlassung in der Europäischen Union hat und Artikel 56 DSGVO im Hinblick auf die Regelungen einer federführenden Aufsichtsbehörde damit nicht anwendbar ist, muss wiederum Artikel 55 Absatz 1 DSGVO zur Anwendung gelangen. Danach ist jede Datenschutzaufsichtsbehörde zuständig, sofern die Verarbeitungstätigkeiten auf betroffene Personen in ihrem Hoheitsgebiet ausgerichtet sind. Ein Unternehmen muss sich also vielmehr überlegen, inwieweit es eine Niederlassung in Europa errichten sollte (im Sinne des „One-Stop-Shop“- Prinzips), um gerade unterschiedliche Verwaltungsverfahren von unterschiedlichen Aufsichtsbehörden zu vermeiden.

B. Sanktionen

Den Aufsichtsbehörden stehen nach der Datenschutzgrundverordnung unterschiedliche Instrumente zur Verfügung, um die Einhaltung von Datenschutz bei den Verantwortlichen und deren Auftragsverarbeitern durchzusetzen. Ein Überblick findet sich im Kurzpapier „Aufsichtsbefugnisse und Sanktionen“ der Datenschutzkonferenz (https://www.lda.bayern.de/media/dsk_kpnr_2_sanktionen.pdf). Diesen Ausführungen ist zu entnehmen, dass es für die Aufsichtsbehörden die Möglichkeit gibt, vorsorgliche Warnungen oder im Falle von Datenschutzverletzungen Verwarnungen (Artikel 58 DSGVO) zusätzlich oder anstelle einer Sanktion in Form einer Geldbuße (Artikel 83 DSGVO) auszusprechen. Bei Nichtbefolgung ihrer Anordnungen kann sie Zwangsgelder verhängen. Eine Aufsichtsbehörde kann zudem erteilte Zertifikate widerrufen.

Die Sanktionen des Artikels 83 DSGVO lassen bei schwerwiegenden Verstößen Geldbußen bis 20 Millionen EURO oder 4% des weltweiten Gesamtumsatzes des vergangenen Geschäftsjahres zu.

Auf europäischer Ebene wurde das noch unter der Artikel-29-Datenschutzgruppe erarbeitete WP 253 „Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679“ inzwischen vom Europäischen Datenschutzausschuss angenommen: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 und https://www.lda.brandenburg.de/media_fast/4055/wp253_de.pdf (deutsch). In diesem Papier wird der Harmonisierungsgedanke nochmals hervorgehoben. Zu diesem Zweck wurden sowohl in Deutschland als auch auf europäischer Ebene Arbeitsgruppen gebildet, um Kriterien für eine einheitliche Sanktionspraxis sicherzustellen. Letztendlich müssen Kriterien für die festzusetzende Höhe einer Sanktion entwickelt werden, etwa dahingehend inwieweit die wirtschaftliche Leistungsfähigkeit eines Unternehmens berücksichtigt werden soll. Teilweise haben die Aufsichtsbehörde geäußert, dass es ihnen zum jetzigen Zeitpunkt nicht vorrangig darum gehe, möglichst viele Fehler zu finden und Bußgelder zu verhängen, sondern stattdessen aufzuklären und zu sensibilisieren (https://www.lfd.niedersachsen.de/startseite/allgemein/presseinformationen/querschnittspruefung_fragen_zur_dsgvo_an_50_unternehmen/fragen-zur-ds-gvo-an-50-unternehmen-166110.html - im Zusammenhang mit der Versendung von Fragebögen zum Stand der Umsetzung der DSGVO an 50 Unternehmen in Niedersachsen).

C. In Kürze

Datenpannen

Bei jeder Datenschutzverletzung besteht immer eine unverzügliche Meldepflicht (binnen höchstens 72 Stunden) an die zuständige Aufsichtsbehörde, es denn der Verantwortliche kann nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt.

Sanktionen

Nach der Datenschutzgrundverordnung sind zwar bei Verstößen Geldbußen bis 20 Millionen EURO oder 4% des weltweiten Gesamtumsatzes des vergangenen Geschäftsjahres vorgesehen. Dennoch stehen den Aufsichtsbehörden grundsätzlich mehrere Möglichkeiten zu, um datenschutzkonformes Verhalten sicherzustellen. Eine Aufsichtsbehörde kann ebenso vorsorgliche Warnungen oder im Falle von Datenschutzverletzungen auch eine Verwarnung anstelle einer Sanktion in Form einer Geldbuße aussprechen.

D. Links und Materialien

- Datenpannen

- **Das Bayerische Landesamt für Datenschutzaufsicht**

  Das Bayerische Landesamt für Datenschutzaufsicht weist in seinem Kurzpapier „Umgang mit Datenpannen“ unter https://www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf darauf hin, dass die Einschätzung dieses Risikos im Alltag eines Unternehmens als große Herausforderung betrachtet werden könnte. Von daher sei zu erwarten, dass sich die Aufsichtsbehörden über die vorzunehmende Risikobewertung näher abstimmen werden.

  In Bezug auf die Benachrichtigung der betroffenen Personen (Artikel 34 DSGVO), die bei einem hohen Risiko für deren Rechte und Freiheiten erfolgen muss, besteht nach Auffassung des Bayerischen Landesamtes für Datenschutzaufsicht Klärungsbedarf dahingehend, wann auf eine solche verzichtet werden kann. Zur Einschätzung eines solchen Risikos stellt die Datenschutzkonferenz ein Kurzpapier zum Download bereit, https://www.lda.bayern.de/media/dsk_kpnr_18_risiko.pdf. (Siehe hierzu auch den nachfolgenden Link der Datenschutzkonferenz).

- **Datenschutzkonferenz**

  Zur Einschätzung eines Risikos für die Rechte und Freiheiten natürlicher Personen stellt die Datenschutzkonferenz ein Kurzpapier zum Download bereit, https://www.lda.bayern.de/media/dsk_kpnr_18_risiko.pdf. Der Begriff des Risikos taucht an mehreren Stellen in der Datenschutzgrundverordnung auf, so auch bei den Regelungen zum Umgang mit einer Verletzung des Schutzes personenbezogener Daten (Artikel 33, 34 DSGVO)

Gemäß den Ausführungen der Datenschutzkonferenz ist Ziel dieses Kurzpapieres, das Risiko im Kontext der DSGVO zu definieren und aufzuzeigen, wie Risiken für die Rechte und Freiheiten natürlicher Personen bestimmt und in Bezug auf ihre Rechtsfolgen bewertet werden können. Die Eindämmung von Risiken durch Ergreifen geeigneter technischer und organisatorischer Maßnahmen sei allerdings nicht Gegenstand des Papiers. Zunächst definiert die Datenschutzkonferenz das Risiko als Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Im weiteren Verlauf des Kurzpapiers erfolgen Ausführungen zu möglichen Schäden, Ereignissen und Risikoquellen, sowie der Hinweis, dass sowohl für die Differenzierung der Eintrittswahrscheinlichkeit als auch für mögliche Schäden jeweils Abstufungen in Form von „geringfügig, überschaubar, substanziell oder groß“ verwendet werden könnten, wobei die Einordnung in die Stufen zu begründen sei. Damit ist gleichermaßen auch die Durchführung einer Datenschutz-Folgenabschätzung erforderlich, da das Risiko einer Datenverarbeitung objektiv ermittelt und beurteilt werden muss. Der Nachweispflicht gemäß Artikel 5 Absatz DSGVO ist dabei besonders Rechnung zu tragen.

- **Artikel-29-Datenschutzgruppe**

  Unter http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827 stellt die Artikel-29-Datenschutzgruppe eine Orientierungshilfe zum Umgang mit Datenschutzverletzungen bereit, unter anderem dahingehend, wann ein solcher Verstoß zu melden ist (wp250rev.01 vom 06. Februar 2018, Guidelines on Personal data breach notification under Regulation 2016/679).

- **Sanktionen**

- **Datenschutzkonferenz**

  Die Datenschutzkonferenz hat ein Kurzpapier zu Befugnissen der Aufsichtsbehörden und deren Sanktionsmöglichkeiten veröffentlicht, abrufbar unter https://www.lda.bayern.de/media/dsk_kpnr_2_sanktionen.pdf.

  Letztendlich bleiben jedoch sowohl die Durchführung in der Praxis als auch mögliche Leitlinien des Europäischen Datenschutzausschusses abzuwarten. Dieses Kurzpapier hat im Übrigen das Kurzpapier zu Sanktionsmöglichkeiten des Bayerisches Landesamtes für Datenschutzaufsicht (https://www.lda.bayern.de/media/baylda_ds-gvo_7_sanctions.pdf) abgelöst.

- **Berliner Beauftragte für Datenschutz und Informationsfreiheit**

  Unter https://www.datenschutz-berlin.de/aufsicht-kontrolle-reform.html gibt die Berliner Landesdatenschutzbeauftragte einen Überblick über Befugnisse der Aufsichtsbehörden.

- **Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen**

  In den FAQ der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen sind erläuternde Ausführungen zu Sanktionsmöglichkeiten der Aufsichtsbehörden enthalten, abrufbar unter https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-

Datenschutzreform/Inhalt/EU-Datenschutzreform/EU-Datenschutzreform__FAQ_/Welche_Sanktionen_und_Durchsetzungsm__glichkeiten_gibt_es_nach_der_DS-GVO_.php

- **Artikel-29-Datenschutzgruppe**

  Die Artikel-29-Datenschutzgruppe hat eine Orientierungshilfe zur Anwendung von Sanktionsmöglichkeiten veröffentlicht. Die englische Fassung steht unter http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 zur Verfügung (Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679 (wp253), 3.Oktober 2017)

  deutsche Fassung: http://www.lda.brandenburg.de/cms/detail.php/bb1.c.545391.de

  Diese Richtlinien wurden zwischenzeitlich vom Europäischen Datenschutzausschuss bestätigt.

  WP 253 führt in Bezug auf die Harmonisierung folgendes aus: „*Although supervisory authorities remain independent in their choice of the corrective measures presented in Article 58 (2), it should be avoided that different corrective measures are chosen by the supervisory authorities in similar cases.*" Allerdings wird ebenso dargestellt, dass *eine genauere Bestimmung der drei Merkmale Wirksamkeit, Verhältnismäßigkeit und abschreckende Wirkung einer Sanktion sich erst entstehenden Datenschutzpraxis der Aufsichtsbehörden sowie im Zuge der Rechtsprechung ergeben wird.*

  Grundsätzlich verweist das WP 253 darauf, dass eine Einzelfallbewertung vorgenommen werden müsste und die Aufsichtsbehörden die am besten geeignete(n) Maßnahme(n) zu bestimmen haben. Darüber hinaus könnten Verstöße gegen die Verordnung, die gemäß Artikel 83 Absatz 4 ihrer Art nach eigentlich in die Kategorie „von bis zu 10.000.000 EURO" fallen würden, können unter bestimmten Umständen auch in eine höhere Kategorie (20 Mio. EURO) eingestuft werden (z.B. nach Nichtbefolgung einer Anweisung). Außerdem müssten auch Zweckbindung und Vereinbarkeit der Nutzung im Rahmen von Artikel 83 Absatz 2 seitens der Aufsichtsbehörden geprüft werden.

- **EU Kommission**

  Die EU-Kommission hat auf ihrer Webseite einen Überblick über Aufgaben der Aufsichtsbehörden und Sanktionsmöglichkeiten veröffentlicht, abrufbar unter https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions_de

- **Information Commissioner (Datenschutzbehörde Isle of Man)**

  Die Datenschutzbehörde der Isle of Man stellt ebenso unter https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/gdpr-in-depth/fines-penalties-and-sanctions/ einen Überblick über Sanktionsmöglichkeiten zur Verfügung.