DSGVO-INFO

DIE UMFASSENDE INFORMATIONSPLATTFORM

STIFTUNG DATENSCHUTZ

DIE DATENSCHUTZAUFSICHTSBEHÖRDEN: MELDEPFLICHTEN UND SANKTIONEN

Juni 2020

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)

Diese Handreichung 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.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf). Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder haben allerdings in ihrem Erfahrungsbericht zur Anwendung der DSGVO darauf hingewiesen, dass die Meldepflicht auf Fälle beschränkt werden sollte, die voraussichtlich zu einem mehr als nur geringen Risiko für die Rechte und Freiheiten natürlicher Personen führen. Dies ist darauf zurückzuführen, dass grundsätzlich jede Datenschutzverletzung der Aufsichtsbehörde zu melden ist und sich die Zahl der Meldungen in der Bundesrepublik Deutschland deutlich erhöht hat. Für die Verantwortlichen bestehe darüber hinaus die Schwierigkeit, einzuschätzen, in welchen Fällen kein Risiko für die Rechte und Freiheiten natürlicher Personen besteht (siehe hierzu unter HTTPS://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/20191209_Erfahrungsbericht-zur-Anwendung-der-DS-GVO.pdf).

Sofern ein Unternehmen keine Niederlassung in der Europäischen Union hat, ist jede Datenschutzaufsichtsbehörde zuständig, sofern die Verarbeitungstätigkeiten auf betroffene Personen in ihrem Hoheitsgebiet ausgerichtet sind. Es gilt das Marktortprinzip mit der Folge, dass jede Behörde zuständig ist. Ein Unternehmen sollte also prüfen, ob die Errichtung einer Niederlassung in Europa zielführend sein könnte (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.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_2.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 von der Artikel-29-Datenschutzgruppe erarbeitete WP 253 „Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679" vom Europäischen Datenschutzausschussbestätigt: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 und https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de. In diesen Leitlinien 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 europaweit Kriterien für die festzusetzende Höhe einer Sanktion entwickelt werden, etwa dahingehend inwieweit die wirtschaftliche Leistungsfähigkeit eines Unternehmens berücksichtigt werden soll. In Deutschland hat die Datenschutzkonferenz, das Gremium der unabhängigen deutschen Aufsichtsbehörden des Bundes und der Länder, ein Konzept zur Bußgeldzumessung in Verfahren gegen Unternehmen entwickelt (https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf). Es soll keine Anwendung auf Geldbußen gegen Vereine oder natürliche Personen außerhalb ihrer wirtschaftlichen Tätigkeit finden. Nach diesem Konzept erfolgt die Bußgeldzumessung in fünf Schritten: „*Zunächst wird das betroffene Unternehmen einer Größenklasse zugeordnet (1.), danach wird der mittlere Jahresumsatz der jeweiligen Untergruppe der Größenklasse bestimmt (2.), dann ein wirtschaftlicher Grundwert ermittelt (3.), dieser Grundwert mittels eines von der Schwere der Tatumstände abhängigen Faktors multipliziert (4.) und abschließend der unter 4. ermittelte Wert anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände angepasst (5.)*."

Die Datenschutzkonferenz verweist allerdings darauf, dass diese Leitlinien nicht erschöpfend sind und die Konkretisierung der Festsetzungsmethodik den späteren Leitlinien des Europäischen Datenschutzausschusses vorbehalten bleibt.

In diesem Zusammenhang soll ergänzend erwähnt werden, dass die Berliner Beauftragte für Datenschutz und Informationsfreiheit in einer Pressemitteilung angekündigt hat, gegen die Deutsche Wohnen SE einen

Bußgeldbescheid in Höhe von 14,5 Millionen Euro wegen Verstößen gegen die Datenschutz-Grundverordnung (DS-GVO) zu erlassen (siehe Pressemitteilung, abrufbar unter

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf). In der Vergangenheit haben die die Aufsichtsbehörden teilweise aber gleichermaßen geäußert, dass es ihnen 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). Es bleibt abzuwarten, inwiefern dieser Beratungsansatz in der Praxis weiterhin zu Tragen kommt. In diesem Sinne hat ebenso das Forum Privatheit in seinem Forschungsbericht "Das Sanktionsregime der Datenschutz-Grundverordnung“ darauf hingewiesen, dass sich eine gewisse Zweigleisigkeit in der Aufsichtspraxis der Behörden unter der Datenschutz-Grundverordnung abzeichnet (siehe unter https://www.forum-privatheit.de/wp-content/uploads/Bericht_DSGVO_Sanktionsregime-1.pdf): Einerseits sei damit zu rechnen, dass der neue Bußgeldrahmen zumindest mittelfristig zu einer schärferen Sanktionierung von Datenschutzverstößen führen werde. Andererseits sei der Spagat zwischen Berater und Aufseher, den die Aufsichtsbehörden dabei zum Teil auszuführen versuchen, nicht einfach und werde viel Kommunikationsgeschick erfordern.

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 stellt auf zwei Übersichtsfolien Hinweise zum Umgang mit Sicherheitsvorfällen zur Verfügung (https://www.lda.bayern.de/media/veroeffentlichungen/Flyer_Datenschutzverletzung.pdf) und erläutert in prägnanter Weise Begriffe wie Cyberattacken, Ransomware und Malware.

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.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.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 2 DSGVO ist dabei besonders Rechnung zu tragen.

Europäischer Datenschutzausschuss

Der Europäische Datenschutzausschuss hat die Leitlinien der Artikel-29-Datenschutzgruppe zum Umgang mit Datenschutzverletzungen bestätigt; siehe wp250rev.01 vom 06. Februar 2018, Guidelines on Personal data breach notification under Regulation 2016/679 (unter anderem zu den Voraussetzungen, wann ein Datenschutzverstoß zu melden ist).

Sanktionen

Forum Privatheit

Forschungsbericht "Das Sanktionsregime der Datenschutz-Grundverordnung“, abrufbar unter https://www.forum-privatheit.de/wp-content/uploads/Bericht_DSGVO_Sanktionsregime-1.pdf)

Datenschutzkonferenz

Die Datenschutzkonferenz hat ein Kurzpapier zu Befugnissen der Aufsichtsbehörden und deren Sanktionsmöglichkeiten veröffentlicht, abrufbar unterhttps://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_2.pdf .

Außerdem hat die Datenschutzkonferenz ein Konzept zur Bußgeldzumessung in Verfahren gegen Unternehmen entwickelt (https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf).

Letztendlich bleiben jedoch 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.

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Zur Verhängung eines Bußgeldes gegen die AOK siehe unter https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-bussgeld-gegen-aok-baden-wuerttemberg-wirksamer-datenschutz-erfordert-regelmaessige-kontrolle-und-anpassung/

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.

Siehe außerdem die Pressemitteilung dieser Behörde zur Verhängung eines Bußgeldes, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf.

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

Europäischer Datenschutzausschuss

Der Europäische Datenschutzausschuss hat die Richtlinien der Artikel-29-Datenschutzgruppe zur Anwendung von Sanktionsmöglichkeiten bestätigt.

Siehe WP 253 „Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679“, abrufbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 und https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de.

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 unter https://www.inforights.im/organisations/old-data-protection-pages/the-general-data-protection-regulation/gdpr-in-depth/fines-penalties-and-sanctions/einen Überblick über Sanktionsmöglichkeiten zur Verfügung.