DSGVO-INFO

DIE UMFASSENDE INFORMATIONSPLATTFORM

STIFTUNG DATENSCHUTZ

Dossier II: Aufsichtsbehörden, Meldepflichten und Sanktionen

Stand: August 2018

Rechtsgrundlage:

Artikel 51 bis 57 Datenschutzgrundverordnung und Erwägungsgründe 117 bis 133, 137 (Zuständigkeit und Aufgaben der Aufsichtsbehörden)

Artikel 58 Datenschutzgrundverordnung und Erwägungsgründe 122, 129, 131 (Befugnisse)

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 den Zuständigkeiten von Aufsichtsbehörden, insbesondere auch bei grenzüberschreitender Datenverarbeitung (A. und B.). In diesem Zusammenhang werden Meldepflichten bei Datenschutzverstößen gegenüber Aufsichtsbehörden behandelt (C.), ebenso unter Beachtung der Sanktionsmöglichkeiten (D.). Unter Punkt E. folgt eine Zusammenfassung. Eine Sammlung mit weiterführenden Links findet sich am Ende der Ausführungen (F.).

A. Zuständigkeiten in Deutschland

Gemäß Artikel 51 Absatz 1 DSGVO sieht jeder Mitgliedstaat vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird.

In Deutschland sind mehrere Aufsichtsbehörden errichtet worden:

- **Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)**

  Die BfDI ist für die Daten- und Informationsverarbeitung aller öffentlichen Stellen des Bundes zuständig, die sie berät und kontrolliert.
  Der BfDI obliegt die Zuständigkeit für nicht-öffentliche Stellen, wenn es sich um Telekommunikations- und Postdienstunternehmen sowie um private Unternehmen handelt, die unter das Sicherheitsüberprüfungsgesetz fallen. Darüber hinaus ist sie die zuständige Aufsichtsbehörde für die Jobcenter. Die BfDI unterrichtet außerdem den Deutschen Bundestag und die Öffentlichkeit über wesentliche datenschutzrelevante Entwicklungen im privatwirtschaftlichen Bereich.

- **Datenschutzbeauftragte der Bundesländer**

  In jedem Bundesland gibt es eine (Landes-)Datenschutzbeauftragte oder einen (Landes-) Datenschutzbeauftragten .

  Die Datenschutzbeauftragten der Bundesländer überwachen bei Behörden und sonstigen öffentlichen Stellen des jeweiligen Bundeslandes die Einhaltung des Datenschutzes (öffentlicher Bereich). Jedes Bundesland hat zudem für die Datenverarbeitung durch öffentliche Stellen der Landesverwaltung und Gemeinden ein eigenes (Landes-)Datenschutzgesetz erlassen.

Werden personenbezogene Daten im nicht-öffentlichen Bereich verarbeitet (z.B. durch Unternehmen, Verbände, Selbstständige und Vereine), kontrolliert die/der zuständige Datenschutzbeauftragte als Aufsichtsbehörde die Einhaltung des Datenschutzrechts in dem Bundesland, in welchem die datenverarbeitende Stelle ihren Sitz hat. Dies gilt allerdings mit Ausnahme von Telekommunikations- und Postdienstunternehmen, für welche die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die zuständige Aufsichtsbehörde ist.

Die Zuständigkeit der Landesbeauftragten erstreckt sich außerdem nicht auf kirchliche Stellen oder den Rundfunk, die eigene Datenschutzbeauftragte haben.

B. Zuständigkeiten bei grenzüberschreitender Datenverarbeitung

Artikel 55 Abs. 1 DSGVO regelt, dass jede Aufsichtsbehörde für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig ist.

Handelt es sich um eine grenzüberschreitende Datenverarbeitung ist Artikel 56 DSGVO einschlägig, wonach die federführende Aufsichtsbehörde als einziger Ansprechpartner des Verantwortlichen zuständig ist. Federführend ist immer die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung in einem europäischen Mitgliedstaat. Liegen diese Voraussetzungen nicht vor, ist wiederum Artikel 55 Absatz 1 DSGVO anwendbar.

Aus Erwägungsgrund 122 und Artikel 55 DSGVO ergibt, dass jede Aufsichtsbehörde dafür zuständig sein sollte, im Hoheitsgebiet ihres Mitgliedstaats die Befugnisse auszuüben und die Aufgaben zu erfüllen, die ihr mit dieser Verordnung übertragen wurden. Dies sollte insbesondere ebenso für Verarbeitungstätigkeiten gelten, die Auswirkungen auf betroffene Personen in ihrem Hoheitsgebiet haben, oder für Verarbeitungstätigkeiten eines Verantwortlichen oder Auftragsverarbeiters ohne Niederlassung in der Union, sofern sie auf betroffene Personen mit Wohnsitz in ihrem Hoheitsgebiet ausgerichtet sind.

Das Zusammenarbeits- und Kohärenzverfahren der Aufsichtsbehörden (Artikel 60 ff. DSGVO) gilt jedoch gemäß den Ausführungen der Artikel-29-Datenschutzgruppe (wp244rev.01- http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48140) nur für Verantwortliche mit einer oder mehreren Niederlassungen in der Europäischen Union, so dass Unternehmen ohne Niederlassung in der Europäischen über ihren lokalen Vertreter mit den zuständigen Aufsichtsbehörden zusammen arbeiten müssen.

C. 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.

D. 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.

Insgesamt werden hierzu Leitlinien des Europäischen Datenschutzausschusses erwartet.

E. In Kürze

Zuständigkeiten in Deutschland

Die Beauftragten der Bundesländer für den Datenschutz sichern das Grundrecht auf Datenschutz:

- Im öffentlichen Bereich überwachen sie im jeweiligen Bundesland, ob die Behörden und sonstigen öffentlichen Stellen, wie z.B. kommunale Krankenhäuser die einschlägigen Datenschutzregelungen (auch die Landesdatenschutzgesetze) einhalten. Zu beachten ist: **Landesdatenschutzgesetze gelten nur für öffentliche Stellen, nicht für private Unternehmen!**

- Im nicht-öffentlichen Bereich kontrollieren sie als Aufsichtsbehörde Unternehmen, die ihren Sitz in dem jeweiligen Bundesland haben. Ausnahme: Telekommunikations- und Postdienstunternehmen. Die

Zuständigkeit der Landesbeauftragten erstreckt sich außerdem nicht auf kirchliche Stellen oder den Rundfunk, die eigene Datenschutzbeauftragte haben.

Regelmäßig sind die Landesdatenschutzbeauftragten zugleich die zuständigen Ansprechpartner für den Datenschutz im nicht-öffentlichen als auch im öffentlichen Bereich. Allerdings sind in Bayern die Behörden getrennt: Der Bayerische Landesbeauftragte für den Datenschutz überwacht die Einhaltung der Datenschutzrechte der Bürger durch die Bayerische öffentliche Verwaltung, während das Bayerische Landesamt für Datenschutzaufsicht als Aufsichtsbehörde für den nicht-öffentlichen Bereich (z.B. Unternehmen) zuständig ist.

Zuständigkeiten bei grenzüberschreitender Datenverarbeitung und Marktortprinzip

Bei grenzüberschreitender Datenverarbeitung ist die federführende Aufsichtsbehörde als einziger Ansprechpartner des Verantwortlichen zuständig ist. Federführend ist immer die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung in einem europäischen Mitgliedstaat.

Hat ein Verantwortlicher weder Hauptsitz noch Niederlassung in der Europäischen Union, sind jedoch die Verarbeitungstätigkeiten auf betroffene Personen mit Wohnsitz in dem jeweiligen Hoheitsgebiet der Aufsichtsbehörde ausgerichtet, darf diese ihre Befugnisse nach der Datenschutzgrundverordnung ausüben.

Insgesamt ist zu beachten. Es gilt europäisches Datenschutzrecht auch ohne Hauptsitz oder Niederlassung des Verantwortlichen in der Europäischen Union, wenn eine Datenverarbeitung im Zusammenhang mit dem Angebot einer (kostenlosen oder kostenpflichtigen) Dienstleistung oder Ware steht oder wenn die Internetaktivitäten von betroffenen Personen durch Cookies oder Browser-Fingerprints nachvollzogen werden können (Marktortprinzip).

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.

F. Links und Materialien

- Aufsichtsbehörden in Deutschland

- **Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)**

  Informationen über die Aufgaben der BfDI sind unter folgendem Link abrufbar:
  https://www.bfdi.bund.de/DE/BfDI/Artikel_BFDI/AufgabenBFDI.html

  Anschriften und Links zu den Datenschutzbeauftragten der Rundfunkanstalten und Kirchen sowie zu den Kontaktdaten von Datenschutzbeauftragten in Europa und weltweit, finden sich unter
  https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

- **Der Bayerische Landesbeauftragte für den Datenschutz und das Bayerische Landesamt für Datenschutzaufsicht**

  Regelmäßig sind die Landesdatenschutzbeauftragten zugleich die zuständigen Ansprechpartner für den Datenschutz im nicht-öffentlichen als auch im öffentlichen Bereich. Allerdings sind in Bayern die Behörden getrennt:

  Der Bayerische Landesbeauftragte für den Datenschutz überwacht die Einhaltung der Datenschutzrechte der Bürger durch die bayerische öffentliche Verwaltung (https://www.datenschutz-bayern.de/).

  Das Bayerische Landesamt für Datenschutzaufsicht ist als Aufsichtsbehörde für den nicht-öffentlichen Bereich (z.B. private Unternehmen) zuständig (https://www.lda.bayern.de/de/index.html#) und stellt einen Flyer mit seinem Aufgabenbereich zum Download zur Verfügung:
  https://www.lda.bayern.de/media/flyer_baylda_organisation_de.pdf .

- **Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg**

  https://www.baden-wuerttemberg.datenschutz.de

- **Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz**

  https://www.datenschutz.rlp.de

- **Der Hessische Datenschutzbeauftragte**

  https://datenschutz.hessen.de

- **Die Landesbeauftragte für den Datenschutz Niedersachsen**

  https://www.lfd.niedersachsen.de

- **Unabhängiges Datenschutzzentrum Saarland**

  https://datenschutz.saarland.de

- **Landesbeauftragte für Datenschutz Sachsen-Anhalt**

  https://datenschutz.sachsen-anhalt.de

- **Berliner Beauftragte für Datenschutz und Informationsfreiheit**

  https://www.datenschutz-berlin.de

- **Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit**

  https://www.tlfdi.de

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

  https://www.ldi.nrw.de

- **Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg**

  http://www.lda.brandenburg.de

- **Die Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern**

  https://www.datenschutz-mv.de

- **Sächsischer Datenschutzbeauftragter**

  https://www.saechsdsb.de

- **Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein**

  https://www.datenschutzzentrum.de

- **Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit**

  https://www.datenschutz-hamburg.de

- **Die Landesbeauftragte für Datenschutz Freie Hansestadt Bremen**

  https://www.datenschutz.bremen.de

- **Zuständigkeiten bei grenzüberschreitender Datenverarbeitung**

- **Das Bayerische Landesamt für Datenschutzaufsicht**

  Das Bayerische Landesamt für Datenschutzaufsicht gibt in dem von ihm erstellten Kurzpapier „One Stop Shop“ einen Überblick über die zuständigen Aufsichtsbehörden bei grenzüberschreitender Datenverarbeitung, https://www.lda.bayern.de/media/baylda_ds-gvo_13_one_stop_shop.pdf . Nach den Ausführungen des Bayerischen Landesamts für Datenschutzaufsicht muss bei der Abgrenzung zwischen Hauptverwaltung als

Hauptniederlassung und einer anderen Niederlassung geprüft werden, wo die Entscheidungen über Zwecke und Mittel einer Verarbeitung getroffen werden. Dabei sei immer die Verarbeitungstätigkeit entscheidend, um die es konkret geht. Dies könne dazu führen, dass es unterschiedliche federführende Aufsichtsbehörden aufgrund unterschiedlicher Tätigkeiten gibt. Die DSGVO führt also nicht automatisch dazu, dass für ein Unternehmen im Rahmen einer grenzüberschreitenden Datenverarbeitung stets die gleiche Datenschutzaufsichtsbehörde tätig ist.

Ein weiteres Kurzpapier „Amtshilfe und gemeinsame Maßnahmen der Aufsichtsbehörden“ des Bayerischen Landesamts für Datenschutzaufsicht (https://www.lda.bayern.de/media/baylda_ds-gvo_14_mutual_assistance.pdf) verweist darauf, dass die in der DSGVO vorgesehenen Formen der Zusammenarbeit insgesamt dazu dienen, bei grenzüberschreitenden Datenverarbeitungen eine einheitliche Anwendung der Verordnung sicherzustellen und enthält Ausführungen dazu, wie diese Zusammenarbeit konkret auszusehen hat und welche Vorgaben zu beachten sind.

- **Datenschutzkonferenz**

  Unter https://www.lda.bayern.de/media/dsk_kpnr_7_marktortprinzip.pdf hat die Datenschutzkonferenz eine Orientierungshilfe zu den Regelungen des Marktortprinzips veröffentlicht. Der Verweis auf dieses Papier erfolgt aus dem Grunde an dieser Stelle unter „Zuständigkeiten der Aufsichtsbehörden“, da berücksichtigt werden muss, dass europäisches Datenschutzrecht auch ohne Hauptsitz oder Niederlassung des Verantwortlichen in der Europäischen Union gilt, wenn eine Datenverarbeitung im Zusammenhang mit dem Angebot einer (kostenlosen oder kostenpflichtigen) Dienstleistung oder Ware steht (Marktortprinzip). Dennoch muss zusätzlich die zuständige Aufsichtsbehörde bestimmt werden. Gerade im Zusammenhang mit Online-Aktivitäten kann eine Vielzahl von Personen in unterschiedlichen Mitgliedsländern betroffen sein.

- **Artikel-29-Datenschutzgruppe**

  Die Artikel-29-Datenschutzgruppe hat unter http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48140 Leitlinien für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters, 05. April 2017 veröffentlicht (wp244rev.01). Der Annex dazu ist abrufbar unter http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48139. Das Zusammenarbeits- und Kohärenzverfahren der Aufsichtsbehörden gemäß der DSGVO gilt gemäß den Ausführungen der Artikel-29-Datenschutzgruppe nur für Verantwortliche mit einer oder mehreren Niederlassungen in der Europäischen Union. Die Artikel-29-Datenschutzgruppe weist darauf hin, dass das bloße Vorhandensein eines Vertreters in einem Mitgliedstaat nicht das Verfahren der Zusammenarbeit und Kohärenz auslöse, sofern das Unternehmen keine Niederlassung in der EU habe. Dies bedeute, dass Verantwortliche ohne Niederlassung in der EU in jedem Mitgliedstaat, in dem sie aktiv sind, über ihren lokalen Vertreter mit den lokalen Aufsichtsbehörden zusammenarbeiten müssen.

- **Data Protection Commissioner (Datenschutzbehörde Irland)**

Ausführungen zur grenzüberschreitenden Datenverarbeitung und federführenden Aufsichtsbehörde http://gdprandyou.ie/cross-border-processing/ sind (englischsprachig) außerdem auf der Webseite der irischen Datenschutzbehörde zu finden.

- **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).

- **ICO: Britische Datenschutzbehörde (Information Commissioner´s Office)**

  Mythen über Pflichten bei Datenpannen sind in den Ausführungen der Britischen Datenschutzbehörde unter https://iconewsblog.org.uk/2017/09/05/gdpr-setting-the-record-straight-on-data-breach-reporting/ (GDPR – setting the record straight on data breach reporting) zu finden.

- **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

- **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.