1 Jahr DSGVO

Entstehung und Ziel

Die DSGVO wurde geschaffen um Daten der Bürger vor den großen – vor allem amerikanischen - Firmen, wie Google zu schützen und deren Persönlichkeitsrechte zu stärken. Bis zu 20 Millionen oder 4% des konzernweiten Umsatzes wurden diesen Firmen angedroht.

Herausgekommen ist ein unklares und komplexes Regelwerk, das Kleinstfirmen genauso trifft wie internationale Konzerne und für große Verunsicherung, Kosten und teilweise Einschränkungen im Tagesgeschäft für alle Firmengrößen bedeutet. Dabei sind die großen amerikanischen Firmen bei ihrer Datensammlung kaum betroffen, weil diese nun über die „freiwillige“ Zustimmung sich das Recht auf die Verarbeitung zusichern. Eine Strafe über 50 Mio an Google wurde von der DSB ausgesprochen – bei 140 Mrd. Umsatz eher ein Tröpfchen.

Datenschutzbehörden und Zahlen

Aber eines ist sicher: Das Bewusstsein für Datenschutz hat sich bei Nutzern erhöht.
Datenschutzbehörde (DSB) Zahl der Beschwerden 2018 verzehnfacht:
- 2017 156 Beschwerden,
- 2018 1.036 Beschwerden, von denen die Hälfte behandelt wurde.
- Bis April 2019 ca. 2000 Beschwerden (laut WKO).

Damit ist auch der Arbeitsaufwand gestiegen, weswegen die DSB in ihrem Jahresbericht schreibt, dass es zusätzliches Personal brauche. Insgesamt wurden rund 140 Verfahren geführt, bei fünf von ihnen kam es zu einer Strafe.

In D:
- 2017 noch im Schnitt 400 Beschwerden und Anfragen pro Monat,
- zwischen Juni und Dezember 2018 mit rund 1370 auf mehr als das Dreifache,
wie aus dem Tätigkeitsbericht des Bundesdatenschutzbeauftragten Ulrich Kelber.

Die zuständigen EU-Behörden haben seit Inkrafttreten der Verordnung rund 144.000 Beschwerden gezählt, in denen die Betroffenen ihre Persönlichkeitsrechte im Internet oder auch sonst im öffentlichen Raum verletzt sahen.

Expertenmeinungen zu 1. Jahr DSGVO

Experten bezweifeln jedoch, dass sich der Datenschutz der Bürger in der Praxis tatsächlich verbessert hat. "Es hat sich, wie erwartet, wenig geändert", sagt der Rechtsinformatiker Nikolaus Forgó. Es gebe immer noch große Rechtsunsicherheit, tatsächlich anders werden Daten der Nutzer nicht behandelt.
- derstandard.at/2000103634477/Ein-Jahr-DSGVO-Ein-wenig-Datenschutz-zu-hohen-Kosten

Stimmen:

Alexandra Vetrovksy-Brychta (iab-austria-Vizepräsidentin): Letztlich war alles nicht schlimm wie befürchtet, zumindest was die Furcht vor Klagen und Beschwerden durch eine falsche oder nicht ausreichend umgesetzte Datenschutz-Grundverordnung, betrifft. Denn die Flut an Klagen durch falsch oder nicht umgesetzte Datenschutz- Grundverordnung (DSGVO) ist bisher ausgeblieben. "Österreich war gut vorbereitet. Vieles der Schwarzmalerei ist nicht eingetreten“. Allerdings sei der Aufwand für die Umsetzung der Datenschutzgrundverordnung deutlich höher gewesen als erwartet.

Peter Schaar (heise.de): „Die europäische Datenschutz-Grundverordnung ist trotz Unsicherheiten ein Erfolg, und ein Beweis für die Handlungsfähigkeit der EU“.

Thilo Weichert (Netzwerk Datenschutzexpertise): „Die Aufsichtsbehörden müssen sich endlich die großen Internetkonzerne vorknöpfen.“

Beata Hubrig (Anwältin): „Wir brauchen Öffentlichkeit für die unangenehmen Folgen von Datenschutzverstößen.“

Ailidh Callander (Privacy International): „Die DSGVO ist das Fundament, nicht die Decke.“

Kirsten Fiedler (European Digital Rights): „Wir sind noch weit davon entfernt, die Datensammlung zu durchblicken.“

Estelle Masse (Access Now): „Die Umsetzung in einigen Staaten ist ein Problem.“

Katarzyna Szymielewicz (Panoptykon Foundation): „Datenschutzbehörden, Zivilgesellschaft und Wissenschaft müssen zusammenarbeiten.“

Benjamin Bergemann (Digitale Gesellschaft): „Den Wächtern des Datenschutzes fehlen die Ressourcen“

Peter Schaar (Europäische Akademie für Informationsfreiheit und Datenschutz): „Der Trend zu immer mehr staatlicher Überwachung ist ungebrochen“

Kerstin Demuth (Digitalcourage): „Wir müssen unsere Rechte auch in Anspruch nehmen.“

Klaus Müller (Verbraucherzentrale Bundesverband): „Das Datenschutzniveau in Europa muss noch besser werden.“

Quelle: https://netzpolitik.org/2019/ein-jahr-datenschutzgrundverordnung-zwoelf-monate-zwoelf-meinungen/

Umsetzung der DSGVO in Unternehmen

KSV-Umfrage hat ergeben:

- 52 % (2018: 28 %) Daten- und IT-Sicherheitsmaßnahmen sind eingeführt oder angepasst.
- 51 % (14) Zustimmungserklärungen zur Datenverarbeitung sind eingeholt, sofern fehlend
- 50 % (30) Es ist geprüft, ob ein Datenschutzbeauftragter nötig ist. Wenn ja, so ist er bereits bestellt.
- 50 % (13) Das geforderte „Verzeichnis der Verarbeitungen“ ist erstellt.
- 48 % (14) Mit Auftragsverarbeitern sind entsprechende vertragliche Vereinbarungen geschlossen oder vorbereitet.
- 45 % (29) Verantwortlichkeiten für Daten- und IT-Sicherheit sind festgelegt und beschrieben.
- 43 % (24) Der Schutzbedarf der verarbeiteten personenbezogenen Daten ist erhoben.
- 43 % (23) Zugriffskontrollmaßnahmen auf personenbezogene Daten sind, sofern nötig, adaptiert.
- 42 % (19) Es ist geprüft, wie Auskunft über die verarbeiteten Daten gemäß DSGVO gegeben werden kann.
- 41 % (17) Personalsensibilisierung und –schulungen zur DSGVO sind durchgeführt.
- 37 % (19) Datenschutz- sowie Daten- und IT-Sicherheitsrichtlinien sind ausgearbeitet.
- 35 % (11) Verträge und Betriebsvereinbarungen sind auf DSGVO-Anforderungen angepasst oder geprüft.
- 31 % (20) Risikoanalysen zu Daten- und IT-Sicherheit sind durchgeführt.
- 22 % (13) Ein Prozess zum Umgang mit Vorfällen wie Datenmissbrauch oder –verlust (Data Breach) ist definiert.
- 9 % (7) Sonstige Maßnahmen
- 10 % (30) Bisher keine Maßnahmen gesetzt/keine im Laufen.

Quelle: https://www.ots.at/presseaussendung/OTS_20190528_OTS0072/ein-jahr-dsgvo-unternehmen-sind-nicht-sicherer-geworden**-anhang**

Persönliche Erfahrung aus Praxis in KMUs:

- Die meisten Firmen haben sich mit der DSGVO beschäftigt

Oft:

- Datenschutzerklärungen auf Homepages aktualisiert
- Informationspflichten online erfüllt
- Hinweis auf Fotos etc. bei Veranstaltungen
- AV-Verträge wurden abgeschlossen
- Einwilligungen (Newsletter oder sonstige Datenverarbeitung)

Selten:

- Verarbeitungsverzeichnis erstellt
- TOMs überprüft und dokumentiert
- Mitarbeiterschulungen regelmäßig?

Sehr selten:

- Datenminimierung?
- Prozesse geändert?
- Automatisches Löschen?
- Prozesse für Databreach, Auskunftsbegehren etc. eingerichtet?

Beantwortung Auskunftsansuchen der Post:

Auskunftsersuchen an Post am 10.01.2019

Antwort am 23.1.2019: „Tatsächlich speichert die Post keine Daten, die Rückschlüsse auf Ihre politischen Ansichten zulassen.„ …

Antwort am 5.2.2019: Bitte um mehr Geduld wegen großer Anzahl an Anfragen

Antwort am 13.2.2019: Bitte um Ausweiskopie

Antwort am 2.4.2019: Auskunft der Post

Enthalten waren die Daten aller Nachsendeaufträge sowie folgende Daten

- Mögliche Zielgruppe für Werbung Bio statistisch hochgerechnet Ja Ja
- Mögliche Zielgruppe Karriereorientiert statistisch hochgerechnet Ja Ja
- Mögliche Zielgruppe Selbstständigkeit statistisch hochgerechnet Ja Ja
- Mögliche Zielgruppe für Werbung Investment statistisch hochgerechnet sehr hoch sehr hoch
- Mögliche Lebensphase statistisch hochgerechnet Paar ohne Kinder Paar ohne Kinder
- Mögliche Zielgruppe für Wahlwerbung SPÖ statistisch hochgerechnet sehr niedrig
- Mögliche Zielgruppe für Wahlwerbung ÖVP statistisch hochgerechnet sehr niedrig
- Mögliche Zielgruppe für Wahlwerbung Neos statistisch hochgerechnet sehr niedrig
- Mögliche Zielgruppe für Wahlwerbung Grüne statistisch hochgerechnet hoch
- Mögliche Zielgruppe für Wahlwerbung FPÖ statistisch hochgerechnet hoch niedrig
- Mögliche Zielgruppe für Werbung Spenden statistisch hochgerechnet niedrig
- Mögliche Zielgruppe für Werbung Distanzhandel erhoben/zugekauft hoch

Sowie Daten von AZ Direct

- Mindestjahreseinkommen/Person in Euro 49.000 Euro
- Lebensphase Person 3 ausbauen, Paar/Familie, Alter bis 49 Jahre oder Kind(er)
- Datenweitergabe Zu Referenzzwecken und statistischen Zwecken
- Dominantes Geo Millieu Performer
- Wahrscheinlichkeitswert Konservative 2.18%
- Wahrscheinlichkeitswert Traditionelle 0.74%
- Wahrscheinlichkeitswert Etablierte 10.9%
- Wahrscheinlichkeitswert Performer 33.25%
- Wahrscheinlichkeitswert Postmaterielle 7.96%
- Wahrscheinlichkeitswert Digitale Individualisten 12.09%
- Wahrscheinlichkeitswert Bürgerliche Mitte 7.85%
- Wahrscheinlichkeitswert Adaptiv Pragmatische 8.42%
- Wahrscheinlichkeitswert Konsumorientierte Basis 6.76%
- Wahrscheinlichkeitswert Hedonisten 9.85%

Sowie einfache Adressdaten ProfileAddress Direktmarketing GmbH

Ein Auskunftsersuchen an AZ Direct wurde ähnlich beantwortet.

Grundlage war das Gewerbe Adresshandel und meine Einwilligung im Zuge eines Adressumzugs.

Einwilligungen als Rechtfertigung zur Datenverarbeitung – Sinn und Unsinn

Für Newsletterversand

Für Haussprechanlagen

Für Versand von Sterbeurkunden von Hinterbliebenen

Für Hausverwaltung zwecks Datenverarbeitung

Für Hotels zwecks Datenverarbeitung

Von Mitarbeitern für die Veröffentlichung von Fotos

Für Ärzte für Einholung einer Kollegenmeinung

Oder für den unverschlüsselten Versand:

Einwilligung zur Übermittlung personenbezogener Daten inkl. Gesundheitsdaten vom Arzt per unverschlüsselter E-Mail gilt als nicht rechtens. Die Abtretung der Verantwortung geeigneter Maßnahmen an den Betroffenen ist lt. Datenschutzbehörde nicht ok

Quelle:
https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181116_DSB_D213_692_0001_DSB_2018_00/DSBT_20181116_DSB_D213_692_0001_DSB_2018_00.pdf

Ein paar Klarstellungen für Anwendungen im Sinne der DSGVO

DSB-Entscheidung SVNR Gesundheitsdatum?

Die DSB hat entschieden, dass die SVNR – mangels Bezug auf den Gesundheits- oder Krankheitszustand – einer natürlichen Person nicht als Gesundheitsdatum iSd Art 4 Z 15 DSGVO bzw. Art 9 Abs 1 DSGVO zu qualifizieren ist.

Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person gehen aus der SVRN nicht (direkt) hervor, sodass diese als schlichtes Datum iSd DSGVO zu qualifizieren ist.

Entscheidend ist– wie bei Bilddaten (vgl. DSB-D202.207/0001-DSB/2018 mwN vom 7. Juni 2018) – der Kontext an, ob ein sensibles Datum iSd Art 9 DSGVO gegeben ist, oder nicht.

Speichern von Ausweiskopien nur in wenigen Fällen erlaubt:

Grundsätzlich sind Sie nicht verpflichtet, eine Kopie Ihres Ausweises vorzulegen oder anderen zu überlassen. Nach § 20 Absatz 2 des Personalausweisgesetzes dürfen nur Sie selbst oder andere Personen mit Ihrer Zustimmung eine Ausweiskopie anfertigen. Diese muss eindeutig und dauerhaft als Kopie erkennbar sein. Mit Blick auf den Grundsatz der Datenminimierung ist aber immer zu fragen, ob es unbedingt einer Kopie des Ausweises bedarf.

Quelle: https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Personalausweis-und-Datenschutz/Datenschutz-und-Personalausweis-2019_06.pdf?mc_cid=9c929f9218&mc_eid=eff05987f2

Weitergabe der E-Mail Adresse an Versanddienstleister?

Bei der Versendung von Paketwaren ist die Weitergabe der Adressdaten des Kunden datenschutzrechtliche zulässig. Bei Speditionswaren ist sogar die Weitergabe der Telefonnummer an die Spedition datenschutzrechtlich erlaubt, da die Telefonnummer erforderlich ist, um einen Liefertermin mit dem Kunden abzustimmen.

DSK: Online-Händler, die Kunden-E-Mail-Adressen an Paketdienstleister zum Zwecke der Übermittlung von „Versandstatus-“ bzw. „Paketankündigungs-„E-Mails weitergeben möchten, dürfen dies unter Geltung der DSGVO nur mit Einwilligung des Betroffenen Kunden vornehmen! Um den datenschutzrechtlichen Vorgaben für die Weitergabe der Kunden- E-Mail-Adressen im ausreichenden Maße nachzukommen, haben Online-Händler im Rahmen des Bestellvorgangs eine transparente Einwilligung des Kunden einzuholen (z.B. durch einen Einwilligungstext mit sogenannter „Check-Box“) und darüber hinaus im Rahmen der Datenschutzerklärung über die Datenerhebung und -weitergabe ausreichend zu informieren.

Die Einholung einer Einwilligung ist auf Plattformen (wie z.B. eBay, Amazon, etc.) nicht möglich, daher sollte in diesen Fällen von der Weitergabe der E-Mailadressen zur (Paket-)Ankündigungszwecken abgesehen werden.

Quelle: https://www.projekt29.de/dsgvo-in-der-praxis-weitergabe-von-e-mailadressen-an-paketdienstleister-dhl-dpd-co-zur-paketankuendigung/

Garantiefall Festplatte mit Daten, was tun?

Wenn ich Daten zur Verarbeitung weitergebe, benötige ich eine Auftragsnehmer-Vereinbarung. Hier stellt sich aber die Frage, ob es sich um eine Datenverarbeitung handelt. Eher nicht – da die Daten eine untergeordnete Rolle im Geschäftsprozess darstellen (ähnlich wie Datenweitergabe an die Post im Zuge eines Versandprozesses). Daher wird wohl keine Auftragsverarbeitung nach Art. 28 notwendig sein, aber eine Vereinbarung zum sorgfältigen/geheimen Umgang mit Daten bzw. der ordnungsgemäßes Entsorgung nach DSGVO. Falls es sich um Daten besonderer Kategorien handelt, würde die Risikoabwägung schon schwieriger ausfallen. Hier würde ich nur Festplatten mit verschlüsselten Daten außer Haus geben.

Anonymisierung als Löschverfahren

Entfernung des Personenbezugs („Anonymisierung“) als Mittel zur Löschung. Im Rahmen des Beschwerdeverfahrens zur GZ: DSB-D123.270/0009-DSB/2018 hatte sich die Datenschutzbehörde mit Bescheid vom 5. Dezember 2018 mit der Frage zu befassen, welche Mittel zur Löschung eingesetzt wer-den können. Der Beschwerdeführer hatte die Löschung sämtlicher Daten begehrt. Die Beschwerdegegnerin entsprach dem Löschbegehren jedoch in der Form, dass sie die Daten des Beschwerdeführers teils faktisch durch Entfernung in ihrem System gelöscht hat, teils hat sie jedoch bloß den Personenbezug zum Beschwerdeführer entfernt (also den Datenbestand des Beschwerdeführers „anonymisiert“). Der Beschwerdeführer brachte im Zuge seiner Beschwerde an die Datenschutzbehörde vor, dass das Primat der faktischen Löschung gelte und er daher in seinem Recht auf Löschung verletzt sei. Die Datenschutzbehörde hat festgehalten, dass dem Verantwortlichen hinsichtlich der Mittel – also der vor-genommenen Art und Weise, wie eine Löschung durch-geführt wird – ein Auswahlermessen zusteht. Da die DS-GVO auf Daten ohne Personenbezug keine Anwendung findet, ist die Entfernung des Personenbezugs (also die „Anonymisierung“) grundsätzlich ein mögliches Mittel, um einem Löschbegehren zu entsprechen. Dabei gilt jedoch ein strenger Maßstab, wonach sichergestellt sein muss, dass weder der Verantwortliche selbst, noch ein Dritter ohne unverhältnismäßigen Aufwand den Personenbezug wiederherstellen kann. Die Beschwerdegegnerin hat im gegenständlichen Fall durch mehrfache Screenshots von ihrem System belegt, dass der Personenbezug entfernt wurde. Darüber hinaus hat die Beschwerdegegnerin den Prozess der Entfernung des Personenbezugs ausreichend und nachvollziehbar dargelegt. Die Beschwerde wurde daher im Ergebnis abgewiesen.

Quelle: https://www.dsb.gv.at/documents/22758/115212/Newsletter_DSB_2_2019.pdf/

Mitverantwortung bei Social Media Plattformen, wie Facebook

EuGH hat am 5.6.2018 (C-210/16) entschieden, dass „jeder Beitrag zum Gelingen einer Datenverarbeitung die datenschutzrechtliche (Mit-) Verantwortlichkeit auslösen kann.

Also wenn man eine Facebook-Fanpage o.ä. einrichtet, mitverantwortlich für die Datenverarbeitung von Facebook ist, auch wenn man die verwendete Technologie nicht beeinflussen kann.

Handlungsempfehlungen der DSK:
- Betroffene transparent informieren inkl. Informationspflichten
- Tracking feststellen und Einwilligung einholen
- Vereinbarung mit Plattformbetreiber abschließen

Wie geht es weiter?

Knyrim: Die deutschen Behörden haben zum Jahresanfang deutlich gesagt, dass die Schonzeit nun vorbei sei. Ich gehe davon aus, dass es in ganz Europa und auch in Österreich heuer bei den Strafhöhen immer öfter ordentlich scheppern wird. Die Aufregung darüber in den Medien wird wieder zu hektischen Reaktionen bei den Unternehmen führen und zu weiteren Hauruck-Aktionen hinsichtlich der Datenschutz-Compliance.

Laut einer EY-Umfrage unter den zuständigen Aufsichtsbehörden erwarten demnach 82 Prozent einen Anstieg bei der Verhängung von Bußgeldern und sonstigen Sanktionen.

Neue Gesetze:

Copyright-Verordnung (Leistungsschutzrecht und Uploadfilter)

Geschäftsgeheimnis-Richtlinie (GeschGehG)

NIS-Richtlinie

Zertifizierungen:

ISO 27001

DSGVO-Zertifikate (offiziell und inoffiziell)

ISO für DSGVO in Planung

Förderungen:

Kein KMU-Digital

Nur noch Förderung im Rahmen Unternehmensberatung:
Modul Einstiegs-Check DSGVO: bis zu max. 4 Stunden à € 80,- pro Stunde zzgl. 20 % USt. Der Zuschuss beträgt € 40,-/Stunde für Unternehmen und € 60,-/Stunde für Jung-unter-nehmen (bis 3 Jahre)
Modul Folgeberatung DSGVO: max. weitere 4 Stunden bei freier Honorarvereinbarung (zw. € 80,- bis max. € 150,-). Der Zuschuss beträgt € 40,-/Stunde für Unternehmen und € 60,-/Stunde für Jung-unter-nehmen (bis 3 Jahre).

Geschäftsgeheimnisgesetz per 1.2.2019:

Das Gesetz sorgt für größere Rechtssicherheit beim Schutz von Geschäftsgeheimnissen. Es setzt eine europäische Richtlinie um (EU 2016/943), die in ganz Europa einen einheitlichen Mindestschutz für Geschäftsgeheimnisse gewährleistet. Davon profitieren Unternehmen, die mit Ideen und Innovationen wirtschaftliche Werte schaffen.

Zugleich wird mit dem Gesetz der investigative Journalismus im Bereich der Geschäftsgeheimnisse gestärkt und es werden erstmals ausdrückliche Regelungen für den Schutz von Hinweisgebern (sog. Whistleblower) geschaffen. Menschen, die Missstände an die Öffentlichkeit bringen, gewinnen dadurch größere Rechtssicherheit.

WAS IST ZU TUN?

Die wichtigste Gesetzesänderung besteht wohl darin, dass Geschäftsgeheimnisse nur noch geschützt sind, wenn angemessene Geheimhaltungsmaßnahmen getroffen sind. In der Vergangenheit war es ausreichend, dass Geschäftsinformationen geheim bleiben sollten. Unternehmen müssen zukünftig ihre angemessenen Schutzmaßnahmen zur Geheimhaltung, damit Informationen auch weiterhin als Geschäftsgeheimnis Schutz genießen, nachweisen können. Es sind also interne Anweisungen und Richtlinien für Mitarbeiter erforderlich.

Welche Maßnahmen genau zu treffen sind, um nachweisen zu können, dass es sich um ein Geschäftsgeheimnis handelt, sagt das Gesetz leider nicht. Als Geheimhaltungsmaßnahmen werden u. a. physische Zugangsbeschränkungen und Vorkehrungen sowie vertragliche Sicherungsmechanismen genannt:

Unternehmen sollten idealerweise immer und überall Geheimhaltung vereinbaren. Unabhängig davon, ob es sich um eine Geschäftsanbahnung, eine Kooperation, Arbeitsverträge oder um Dienstleistungsverträge handelt.

Technische Maßnahmen: Hier kann man sich u. a. am Datenschutz-Managementsystem orientieren wie z. B. Maßnahmen zur Zutritts-, Zugriffs- und Zugangskontrolle

Organisatorische Maßnahmen: Es sollte sichergestellt sein, dass nur Beschäftigte vertrauliche Informationen kennen und zu diesen Zugang haben, die für ihre Tätigkeit benötigt wird (z. B. Berechtigungskonzept, Zugriffsmatrix).

Risikobeurteilung

- DSFA notwendig

- TOMs

- Meldung an DSB bei Datenschutzverletzung
  Nicht jede Datenschutzverletzung löst die Meldepflicht nach Art. 33 DSGVO oder die Benachrichtigungspflicht nach Art. 34 DSGVO aus. Beide Pflichten sind Reaktionen auf das Entstehen von Risiken für die Rechte und Freiheiten natürlicher Personen, und zwar in erster Linie der von einer Verletzung des Schutzes ihrer personenbezogenen Daten betroffenen Personen. Die Meldepflicht gegenüber der Datenschutz-Aufsichtsbehörde greift bereits bei einem niedrigen Risikoniveau ein, während die Benachrichtigungspflicht gegenüber betroffenen Personen ein hohes Risikoniveau voraussetzt. Die Meldepflicht nach Art. 33 Abs. 1 Satz 1 DSGVO entsteht nicht, wenn die Verletzung „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“. Demgegenüber sind betroffene Personen nach Art. 34 Abs. 1 DSGVO (nur dann) zu benachrichtigen, wenn die Verletzung „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge [hat]“.
  Zu unterscheiden sind danach drei Risikostufen:

    - Tritt voraussichtlich kein Risiko auf – in der Sache handelt es sich um ein vernachlässig-bar geringes(datenschutzrechtlich nicht relevantes) Risiko –, unterbleiben sowohl die Meldung einer Datenschutzverletzung an die Datenschutz-Aufsichtsbehörde wie auch die Benachrichtigung der betroffenen Personen.–
    - Entsteht voraussichtlich ein (datenschutzrechtlich relevantes)Risiko, ist nach Art. 33 Abs. 1 DSGVO zu melden, aber nicht nach Art. 34 Abs. 1 DSGVO zu benachrichtigen.
    - Nur wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko zur Folge hat, muss eine Meldung an die Datenschutz-Aufsichtsbehörde abgegeben werden und es müssen auch die betroffenen Personen benachrichtigt werden

Quelle: https://www.datenschutz-bayern.de/datenschutzreform2018/OH_Meldepflichten.pdf?mc_cid=9c929f9218&mc_eid=eff05987f2

ToDo's für Dienstleistung und Anwender

DSGVO Umsetzungen überprüfen – am besten bei einer jährlichen Überprüfung auf die Notwendigkeiten hinweisen bzw. einen Umsetzungsplan erarbeiten.

- Dokumentationspflichten
- Verträge / Vereinbarungen
- Informationspflichten (Trennung von Art. 13 und Art. 14)
- Löschpflichten
- Datenminimierung
- Prozesse anpassen
- TOMs insbes. Einschränkungen bei Zugriff und Verschlüsselung

Mitarbeiter schulen (Kunden und Mitarbeiter)

Privacy by Design in alle Projekte und Überlegungen einbeziehen

Weitere Compliance-Themen w.o. in Überlegungen einbeziehen

Risikomanagement als übergeordnete Disziplin verstehen