TÜV AUSTRIA

AKADEMIE

Erfolgreich als Datenschutzbeauftragter

TÜV AUSTRIA Fachverlag

IMPRESSUM

Erfolgreich als Datenschutzbeauftragter

1. Auflage

ISBN 978-3-903255-11-1

Autoren: Mag. iur. Agata Facco, Mag. iur. Sabine Gölles, MA,
Univ. Lekt. Nicolas Nagel, CIPP/E, CIPM, FIP,
Mag. iur. Michael Tanzberger, TÜV TRUST IT TÜV AUSTRIA GMBH

Medieninhaber
TÜV AUSTRIA AKADEMIE GMBH
Leitung: Mag. (FH) Christian Bayer, Rob Bekkers, MSc BSc
2345 Brunn am Gebirge, TÜV AUSTRIA-Platz 1
+43 5 0454-8000
akademie@tuv.at | www.tuv-akademie.at

Produktionsleitung:
Mag. Judith Martiska
Layout, Satz und Grafiken: Markus Rothbauer, office@studio02.at,
Lukas Drechsel-Burkhard, luc@luc.at
Herstellung: druckwelten.at
Cover: Fotolia

Produziert nach den Richtlinien des Österreichischen Umweltzeichens, UZ 24 Druckerzeugnisse.
UW 750 – sandler print & packaging

INHALT

1. EINLEITUNG

1.1 Lernziele

Die Artikel 37 bis 39 der EU-DSGVO beschreiben die Benennung, Stellung und Aufgaben des/der Datenschutzbeauftragten. Zu den Aufgaben zählen unter anderem die Information und Beratung der Führungskräfte und Beschäftigten, die Überwachung der Einhaltung der DSGVO und weiterer gesetzlicher Grundlagen sowie die Zusammenarbeit mit Behörden.

Dieses Skriptum vermittelt Ihnen folgende Lernziele für Ihre Aufgabe als Datenschutzbeauftragte/r:

- ✓ Verschaffen eines strukturierten Überblicks über die DSGVO
- ✓ Anwendungshilfe in der Praxis
- ✓ Erweitertes Verständnis für die Bereiche Informationssicherheit, IT-Sicherheit und Arbeitsrecht

1.2 Wie nutze ich dieses Skriptum?

Dieses Skriptum begleitet die Ausbildung zum/r zertifizierten Datenschutzbeauftragten TÜV® und ist entsprechend den Lehrinhalten aufgebaut.

Besonders wichtige Inhalte sind in Merkkästen zusammengefasst.

Häufige Fragen zum Datenschutz und zur Informationssicherheit aus dem beruflichen Alltag werden praxisnah und mit Beispielen beantwortet.

Ergänzt werden die Kapitel durch Übungsbeispiele, in denen das Gelernte direkt praktisch umgesetzt werden kann.

2. GRUNDLAGEN DATENSCHUTZ

Zwischen Datenschutz und Datensicherheit besteht ein erheblicher Unterschied. Die beiden Begriffe werden in der Praxis leider oftmals verwechselt.

Was ist Datenschutz?

Datenschutz hat zum Ziel, den Menschen und Informationen (oder Daten) über diesen zu schützen.

Sichergestellt wird dies über die unterschiedlichsten nationalen und internationalen Normen und Gesetze. Dazu gehören insbesondere:

- ✓ EU-Datenschutzgrundverordnung (EU-DSGVO)[1]

  Die DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.
- ✓ Österreichisches Datenschutzgesetz (DSG)[2]
- ✓ Charta der Grundrechte der Europäischen Union (GRC)[3], insbesondere Art 8

  Die GRC gilt für jegliche Art der Datenverarbeitung.
- ✓ Europäische Menschenrechtskonvention (EMRK)[4], insbesondere Art 8

Das Recht auf Datenschutz ist das informationelle Selbstbestimmungsrecht eines jeden Menschen.

Beim Datenschutz geht es um **personenbezogene** Daten und den Schutz des dahinterstehenden **Menschen** vor Missbrauch während Erhebung, Verarbeitung und Nutzung dieser Daten.

Was ist Datensicherheit?

Datensicherheit hat hingegen zum Ziel, schlicht Daten zu schützen, unabhängig von ihrer Einstufung als personenbezogen oder nicht personenbezogen.

Datensicherheit gilt dabei als Teilaspekt des Datenschutzes.

Schutzzwecke sind:

- ✓ die Vertraulichkeit (nur autorisierte Nutzer haben Zugang zu Daten)

1 Vgl. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE
2 Vgl. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597
3 Vgl. http://www.europarl.europa.eu/charter/pdf/text_de.pdf
4 Vgl. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000308

- ✓ die Integrität (Schutz vor beabsichtigten oder unbeabsichtigten Veränderungen)
- ✓ die Verfügbarkeit (Gewährleistung des ständigen Zugriffs auf die Daten) und
- ✓ die Kontrollierbarkeit (Prüfung der Maßnahmen durch Protokollierung)

Datensicherheit hat zum Ziel, **beliebige** Daten vor Schäden, wie Manipulation und Nicht-Verfügbarkeit, zu schützen.

Hierzu zählen Aspekte wie

- ✓ physische Sicherheit,
- ✓ der Schutz vor Fremdzugriffen,
- ✓ die Datensicherung,
- ✓ der Schutz vor internen Zugriffen,
- ✓ das Pflegen von Updates und Patches,
- ✓ die Verschlüsselung der Kommunikation und Datensicherheit.

Was ist technisch möglich?

Der Algorithmus von „Cambridge Analytica“ kann nach eigenen Angaben mit 68 Informationen über Sie (z. B. „Likes“ auf Facebook) mit einer Wahrscheinlichkeit von 90–95 % folgende Informationen zu Ihrer Person eruieren:

- ✓ Hautfarbe,
- ✓ sexuelle Orientierung,
- ✓ politische Zugehörigkeit,
- ✓ Gesundheit,
- ✓ finanzieller Status,
- ✓ und viele weitere

So gut kann Sie der Algorithmus anhand der Informationen über Sie einschätzen:

♥♥♥♥♥♥♥

Bei 70 Likes: besser als Ihre Freunde

♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥

Bei 150 Likes: besser als Ihre Eltern

♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥♥

Bei 300 Likes: besser als Ihr Partner

♥♥♥

Bei 350 Likes: besser als Sie selbst

Wie gut wird er Sie wohl anhand folgender Merkmale einschätzen können?

- ✓ gesendete Inhalte in WhatsApp
- ✓ Bestellungen auf Amazon
- ✓ Suchanfragen in Google
- ✓ App-Daten vom Smartphone
- ✓ geschriebene E-Mails
- ✓ Inhalte Ihrer Google- oder Apple-Cloud
- ✓ Fotos
- ✓ Ebay- und Willhaben-Inserate usw.

Welche Erkenntnisse können bereits jetzt über uns gesammelt und analysiert werden?

„Cracked Labs“, das Institue of Critical Digital Culture, hat dies am Beispiel Acxiom beeindruckend dargelegt:[5]

Acxiom stellt mehr als 3 000 Merkmale und Wertungslisten für 700 Millionen Menschen in den USA, Europa und weiteren Regionen zur Verfügung, unter anderem:

- ✓ Alter, Geschlecht, Ausbildung
- ✓ Religion, ethnische Herkunft
- ✓ Beschäftigungsverhältnis, Einkommen, Eigenkapital, Kredite
- ✓ Details über Bank- und Versicherungsverträge
- ✓ Einkäufe, u. a. die Anzahl der mittels Kreditkarte getätigten Einkäufe der letzten 24 Monate
- ✓ Medienkonsum, Aktivitäten
- ✓ Immobilien- und Fahrzeugbesitz, Details über die Wohnsituation
- ✓ politische Ansichten
- ✓ Beziehungsstatus, Anzahl der Kinder bzw. Kinderwunsch

Wie wird man identifiziert?

Über folgende Daten ist eine Identifizierung möglich:

- ✓ Geräte-ID
- ✓ E-Mail-Adresse
- ✓ Telefonnummer
- ✓ Postanschrift
- ✓ Name, Geschlecht, Geburtsdatum, PLZ
- ✓ Sozialversicherungsnummer

5 Vgl. https://crackedlabs.org/en/corporate-surveillance

- ✓ Kreditkartennummer
- ✓ Google-ID, Facebook-ID, Microsoft-ID, Apple-ID, Amazon-ID etc.

Über diese Daten können Nutzer über Websites, Plattformen und Endgeräte nachverfolgt werden:

- ✓ Cookie-IDs
- ✓ Fingerprints auf mobilen Geräten oder Browsern
- ✓ IP-Adresse

Folgende weitere Daten des Nutzerverhaltens werden zur Identifikation genutzt:

- ✓ besuchte Websites
- ✓ benutzte Apps
- ✓ Videos
- ✓ besuchte Orte
- ✓ hinzugefügte Kontakte
- ✓ Kaufverhalten

Welche Datenmengen werden generiert?

Daten sind in der heutigen Zeit nicht nur Kern jedes Prozessablaufes und von IT-Systemen, sondern vor allem auch etwas wert.

Die generierten Datenmengen nehmen dabei von Jahr zu Jahr exponentiell zu und der weltweite Datenbestand verdoppelt sich alle 2 Jahre!

Statistiken zum Nachdenken:

- ✓ Die gesamte weltweite Datenmenge vom Jahr 0 bis 2016 entspricht jener Datenmenge der Jahre 2016 bis 2018.
- ✓ Bald werden 50 Milliarden Geräte mit dem Internet verbunden sein.
- ✓ Der durchschnittlich vernetzte Mensch wird 4 800-mal täglich in irgendeiner Form mit internetverknüpften Geräten interagieren.
- ✓ Täglich werden Daten erzeugt, welche einer Speicherkapazität von 36 Millionen iPads entsprechen.
- ✓ Der prognostizierte Datenbestand für 2025: ca. 160 Zettabytes = 100 Millionen-mal die Strecke Erde <–> Mond mit gestapelten DVDs

Übersicht Speichergrößen

1 000 Megabytes	=	1 Gigabyte
1 000 Gigabytes		1 Terabyte
1 000 Terabytes		1 Petabyte
1000 Petabytes		1 Exabyte
1 000 Exabytes		1 Zettabyte
1 000 Zettabytes		1 Yottabyte

Wie viele Daten werden pro Minute generiert?

Hier ein paar Beispiele bekannter Anbieter:[6]

- LinkedIn: 120 neue Mitglieder
- Snapchat: 2 083 333 geteilte Snaps
- YouTube: 4 333 560 Videos
- Twitter: 473 400 Tweets
- Textnachrichten: 12 986 111
- Skype: 176 220 Anrufe
- Instagram: 49 380 Fotos
- Spotify: 750 000 Songs
- Tinder: 6 940 Matches
- Google: 3 877 140 Suchanfragen
- Amazon: 1 111 versendete Pakete
- Uber: 1 389 Fahrten

Ist Datenschutz etwas gänzlich Neues?

Auch wenn für manche Unternehmen und Organisationen Datenschutz etwas Neues darstellt, so gibt es Gesetze diesbezüglich schon seit vielen Jahrzehnten – in Österreich konkret seit dem Jahr 1978. Im Jahr 1995 wurde dann die EU-Richtlinie zum Datenschutz erlassen, welche im Jahr 2000 ihre Ausgestaltung im Datenschutzgesetz 2000 (DSG 2000) erfuhr.

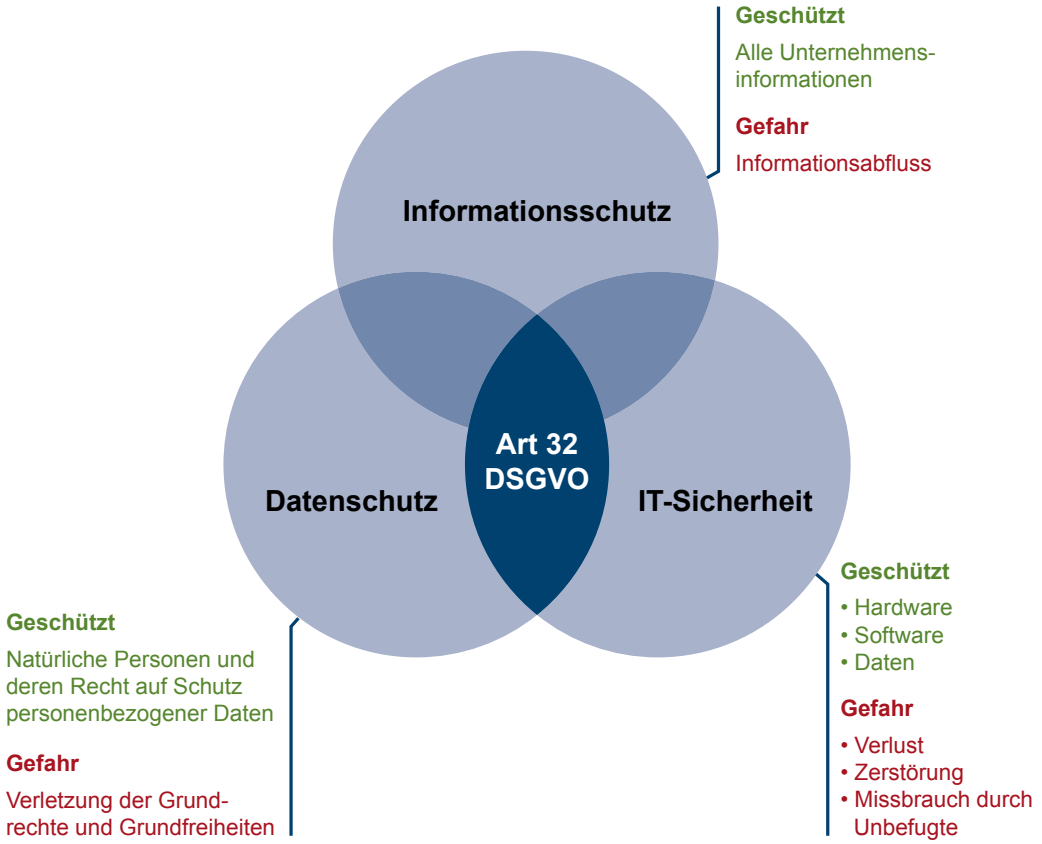
Durch die Datenschutzgrundverordnung wurde der Datenschutz dann europaweit einheitlich und direkt anwendbar geregelt.

6 Vgl https://www.domo.com/learn/data-never-sleeps-6

Die DSGVO trat am 25.05.2016 in Kraft und erlangte ihre Geltung am 25.05.2018.

Welcher Zusammenhang besteht mit Informationssicherheit und IT-Sicherheit?

Um Daten schlussendlich ausreichend schützen zu können, bedarf es jedoch nicht nur der Berücksichtigung des Datenschutzes, sondern auch der verwandten Themenbereiche Informationssicherheit und IT-Sicherheit.



Plakativ lässt sich dies anhand des folgenden Szenarios darstellen:

Ziel: Schutz von Daten!	**DATENSCHUTZ** Sie wissen unter Umständen, dass es eine rechtliche Vorgabe gibt, welche vorsieht, dass personenbezogene Daten geeignet geschützt werden müssen.
	INFORMATIONSSICHERHEIT Sie legen fest, dass eine technische Schranke vor unberechtigtem Zugriff vorhanden sein muss und ein Prozess definiert wird, um die Vertraulichkeit sicherzustellen.
	IT-SICHERHEIT Sie definieren, dass der Verschlüsselungsalgorithmus „AES 256“ zur Absicherung der gespeicherten Daten verwendet werden muss.

3. ÜBERBLICK ZUR DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Im Dezember 2015 erfolgte die Einigung der Europäischen Union auf eine Reform des Datenschutzrechts. Das Ergebnis war die Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, die wir nun alle besser kennen als EU-Datenschutzgrundverordnung oder kurz DSGVO.

Nach Zustimmung des Europäischen Parlaments ist die DSGVO am 4. Mai 2016 im EU-Amtsblatt veröffentlicht worden und damit 20 Tage später **am 25. Mai 2016 in Kraft getreten.**

Ihre **Wirkung bzw. Geltung** entfaltete diese zwei Jahre nach dem Inkrafttreten der Verordnung am **25. Mai 2018.**

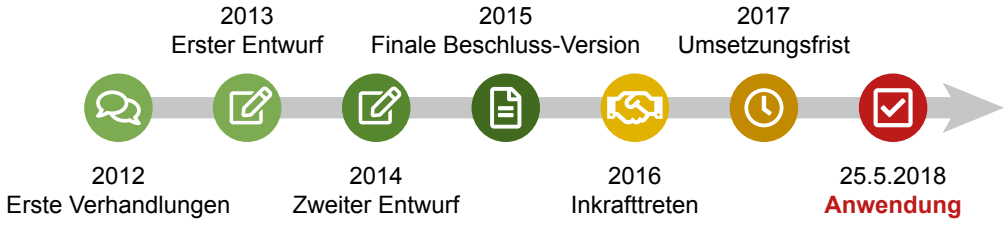
Ist eine Neuregelung des Datenschutzes überhaupt notwendig gewesen?

Die europäischen Datenschutzgesetze gingen zurück auf die EU-Datenschutzrichtlinie aus dem Jahr 1995. EU-Richtlinien wirken nicht unmittelbar und müssen von jedem Mitgliedstaat umgesetzt werden. Dies führte im Ergebnis zu 28 verschiedenen Datenschutzgesetzen in Europa und einem uneinheitlichen Schutzstandard der EU-Mitgliedstaaten, der weder den Verbrauchern oder Bürgern half, noch den datenverarbeitenden Unternehmen und Organisationen sinnvoll zur Seite stand.

In Österreich war dies das Datenschutzgesetz 2000 (DSG 2000).

Ständig herrschte die Frage vor: „Was gilt denn jetzt wo, wann und wie?“

Wie war der Zeitplan zur DSGVO?



Was passierte mit geltendem Recht am 25.5.2018?

Die Datenschutzrichtlinie der EU wurde mit Anwendung der DSGVO aufgehoben. Das gleiche Schicksal ereilte das österreichische DSG 2000.

Die DSGVO räumt den Mitgliedstaaten über sogenannte Öffnungsklauseln jedoch eigene Umsetzungsspielräume ein. Dies betrifft unter anderem:

- ✓ den Beschäftigtendatenschutz
- ✓ das Einwilligungsalter von Jugendlichen in Dienste der Informationsgesellschaft
- ✓ Datenschutzbeauftragte

Für Österreich gilt seit 25.05.2018 nunmehr das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG).[7]

Die gleiche Situation stellt sich in den anderen EU-Mitgliedstaaten dar. Damit wird Datenschutz weiterhin nicht ganz einheitlich innerhalb der EU geregelt sein – ein wichtiger Schritt hin zur Harmonisierung erfolgte damit jedoch.

Das DSG beinhaltet diesbezüglich Sonderregeln zu den Themen:

- ✓ Einwilligungsalter von Jugendlichen
- ✓ Stellung Datenschutzbeauftragter
- ✓ Datengeheimnis
- ✓ Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke
- ✓ Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen
- ✓ Freiheit der Meinungsäußerung und Informationsfreiheit
- ✓ Verarbeitung personenbezogener Daten im Katastrophenfall
- ✓ Bildverarbeitung

Wofür gilt die DSGVO?

Die DGSVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen,

- ✓ im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union, unabhängig davon, ob die Verarbeitung in der Union stattfindet.
- ✓ durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung betroffene Personen, die sich in der Union befinden, betrifft und Waren oder Dienstleistungen angeboten werden oder das Verhalten betroffener Personen beobachtet wird.

7 Vgl. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597

Ausnahmen sind für bestimmte Tätigkeiten vorgesehen:

- ✓ im Rahmen der nationalen Sicherheit
- ✓ durch Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung
- ✓ durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (z. B. Adressbücher, Social Media)
- ✓ Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der EU

Welche Strafen gibt es für Verstöße?

Geldbußen für Verstöße gegen die DSGVO müssen im jeweiligen Einzelfall **wirksam, verhältnismäßig und abschreckend** sein.Diese werden zusätzlich oder an Stelle von weiteren Maßnahmen (z. B. Untersagung der Datenverarbeitung) verhängt.

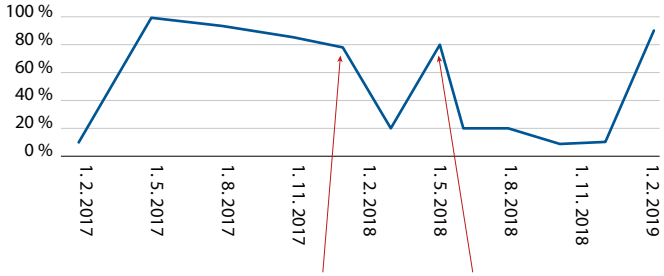
Bei Verstößen gegen die Bestimmungen der DSGVO können Geldbußen von bis zu € 20 000 000,– oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist.

Faktoren für die Bemessung der Geldbußen sind:

- ✓ Art, Schwere und Dauer des Verstoßes
- ✓ Zahl der von der Verarbeitung betroffenen Personen und das Ausmaß des von ihnen erlittenen Schadens
- ✓ Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind
- ✓ Vorsätzlichkeit oder Fahrlässigkeit
- ✓ getroffene Maßnahmen zur Minderung des entstandenen Schadens
- ✓ etwaige einschlägige frühere Verstöße
- ✓ Umfang der Zusammenarbeit mit der Aufsichtsbehörde
- ✓ Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde
- ✓ Einhaltung von genehmigten Verhaltensregeln oder genehmigten Zertifizierungsverfahren
- ✓ jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall

DSGVO-Trend in Österreich

Interesse an der DSGVO

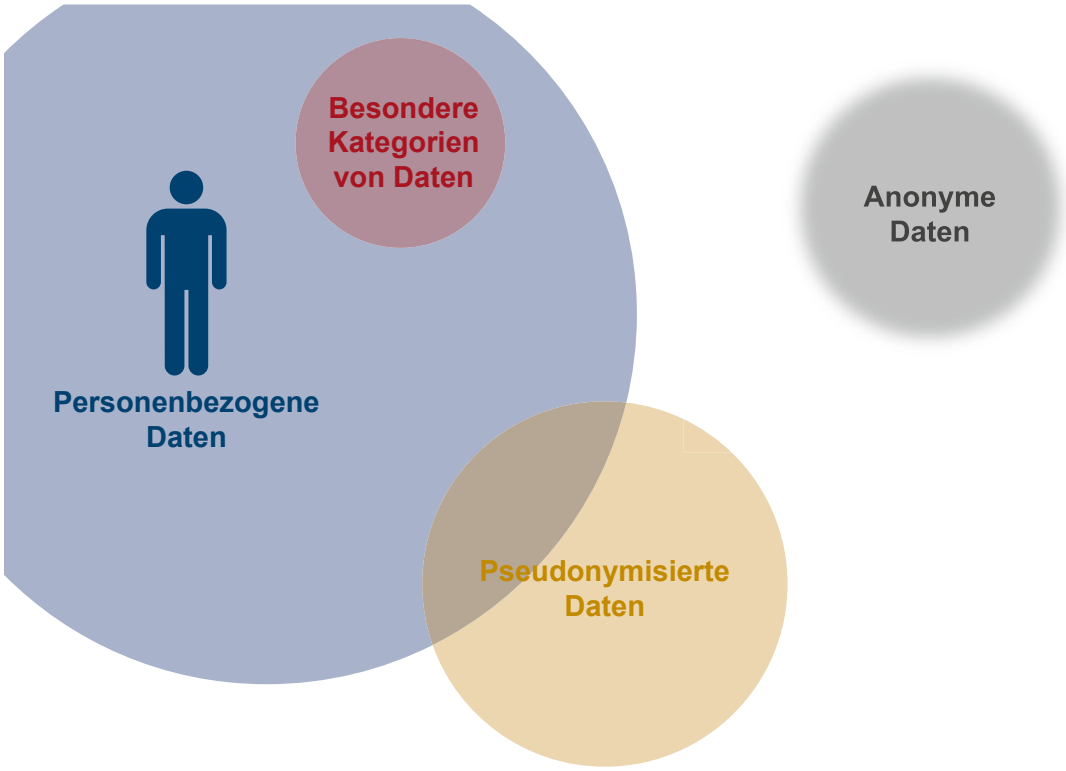


über 1 000 Beschwerden
über 300 Meldungen von DS-Verletzungen
über 150 laufende Verwaltungsstrafverfahren
über 1 000 Beratungsanfragen
Meldung von über 5 000 DS-Beauftragten
Tendenz stark steigend

„Es wird nicht gestraft, nur beraten."

Ende der Umsetzungsfrist Mai 2018

4. GRUNDBEGRIFFE DER DSGVO



Welche Kategorien von Daten gibt es?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen.

Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung, wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann (z. B. IP-Adresse).

Anonyme Daten lassen hingegen faktisch keinen Rückschluss auf eine individuelle Person mehr zu.

Pseudonymisierte Daten werden in einer Weise verarbeitet, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Die Pseudonymisierung ist eine gebotene Maßnahme zur Risikominimierung, die DSGVO gilt aber auch weiterhin.

Illustrieren wir dies anhand des folgenden Beispiels. Stellen Sie sich ein Excel-Dokument wie folgt vor:

Direkt personenbezogen

Nr	Name	Personalnummer	Gehalt
1	Michael Muster	AT 718290	5000
2	Markus Steiner	AT 862652	4500
3	Hanna Ebner	AT 554872	4800
4	Karl Müller	AT 678619	3900
5	Christine Stabner	AT 798784	6100

Indirekt personenbezogen

Nr	Name	Personalnummer	Gehalt
1		AT 718290	5000
2		AT 862652	4500
3		AT 554872	4800
4		AT 678619	3900
5		AT 798784	6100

Anonym

Nr	Name	Personalnummer	Gehalt
1			5000
2			4500
3			4800
4			3900
5			6100

Pseudonymisiert

Dateibesitzer personenbezogen

Nr	Name	Personalnummer	Gehalt
1	Michael Muster	AT 718290	5000
2	Markus Steiner	AT 862652	4500
3	Hanna Ebner	AT 554872	4800
4	Karl Müller	AT 678619	3900
5	Christine Stabner	AT 798784	6100

pseudonymisiert ▼

anonym Dateiempfänger

Nr	Name	Personalnummer	Gehalt
1			5000
2			4500
3			4800
4			3900
5			6100

Besondere Kategorien personenbezogener Daten sind hingegen taxativ durch die DSGVO aufgelistet:

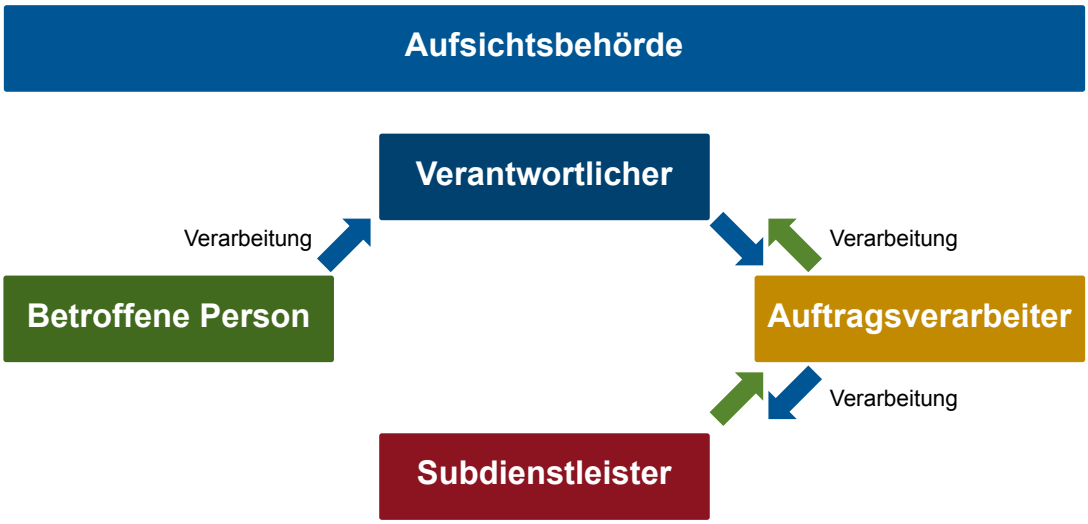
- ✓ rassische und ethnische Herkunft
- ✓ politische Meinungen
- ✓ religiöse oder weltanschauliche Überzeugungen
- ✓ Gewerkschaftszugehörigkeit
- ✓ genetischen Daten
- ✓ biometrischen Daten
- ✓ Gesundheitsdaten
- ✓ Daten zum Sexualleben oder der sexuellen Orientierung

Die Verarbeitung dieser Daten bewirkt dabei erhöhte Dokumentations- und Sorgfaltspflichten. Bildaufnahmen zählen jedoch nicht automatisch dazu, nur weil unter Umständen o. a. Informationen ersichtlich sind (z. B. Hautfarbe, körperliche Beeinträchtigung).

Welche „Rollen“ gibt es im Datenschutz?

Bei den „Rollen“ des Datenschutzes ist zwischen folgenden zu unterscheiden:

- ✓ **Verantwortliche**
  die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet
- ✓ **Auftragsverarbeiter**
  eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet
- ✓ **Betroffene Person**
  die natürliche Person, deren personenbezogenen Daten verarbeitet werden
- ✓ **Empfänger**
  eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger.
- ✓ **Verarbeiten von Daten**
  jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder der Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung



5. FALLPRÜFUNGSSCHEMA DATENSCHUTZ

Um eine strukturierte und geordnete datenschutzrechtliche Prüfung von Sachverhalten vornehmen zu können, empfiehlt es sich, ein Fallprüfungsschema[8], wie folgt dargestellt, einzuhalten.

Die Prüfung erfolgt dabei Schritt für Schritt auf Einhaltung der Bestimmungen der DSGVO.

Zur besseren Darstellung und Nachvollziehbarkeit erfolgt die Struktur der nachfolgenden Kapitel in Analogie zum Fallprüfungsschema.

8 Vgl. Nagel, Praxishandbuch Datenschutz, Leitfaden zur DSGVO für Juristen und Laien, TÜV AUSTRIA Fachverlag 2019