DIE TECHNISCHE SEITE DES DATENSCHUTZES

DS BY DESIGN, DS BY DEFAULT, DS-FOLGEABSCHÄTZUNG

MICHAEL MORGENTHALER

- Seit 10/2020 Selbständig mit Beratung/Vorlesung/DSgzS
- 2007 – 09/2020 Datenschutz-Beauftragter (stv.), SAP SE
- 2001 – 2006 Information Security Manager, SAP SE
- 2009 – 2015 im Vorstand ISACA Germany Chapter
- Zertifizierungen:
  - Certified Data Privacy Solutions Engineer (CDPSE) – ISACA (+ Trainer)
  - Certified Information Privacy Professional (CIPP/E) – IAPP
  - Certified Information Privacy Technologist (CIPT) – IAPP
  - Fellow of Information Privacy (FIP) -IAPP
  - Datenschutz-Auditor (TÜV)
  - Certified Information System Auditor (CISA) – ISACA
  - Certified Information Security Manager (CISM) – ISACA
- morgenthaler@dsb-mm.de

VORBEMERKUNG

- Inhalte in diesem Vortrag dienen lediglich Informationszwecken.
- Sie stellen keine Rechtsberatung dar.
- Sie können insbesondere keine individuelle rechtliche Beratung ersetzen, welche die Besonderheiten des Einzelfalles berücksichtigen.
- Sie beinhalten keine Aussagen bzgl. meiner Arbeitgeber oder Mandanten.

AGENDA

- Die Datenschutz-Grundverordnung
- Neue Prinzipien bei der SW-Entwicklung und Betrieb
  - Privacy by Design
  - Privacy by Default
- Datenschutz-Folgeabschätzung
- Fazit

Quelle: pixabay.com Gerd Altmann

Die Datenschutz-Grundverordnung (DSGVO)

DIE DATENSCHUTZ-GRUNDVERORDNUNG

- VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES
  zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (**Datenschutz-Grundverordnung/DSGVO**)

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation/GDPR**)

DSGVO HISTORIE

- 1995 Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
  - BDSG, DP Act 1998 (UK), LOI 2004-80 (F),..
- Ab 2012 in der politischen Diskussion
  - Starke Einflussnahme von (US) Lobbyisten
- 2016 Verabschiedet, enthält viele Elemente des BDSG
- Seit 2018 (mit lokalen Öffnungsklauseln) anzuwenden

WAS IST UNVERÄNDERT / WAS IST NEU?

- Verordnung, keine Richtlinie (neu)
- Personenbezogene Daten
- Verarbeitung grundsätzlich verboten, nur aufgrund abschließender Erlaubnistatbestände
- Bestellung Datenschutzbeauftragter (verändert)
- Marktort-Prinzip/Territoriale Reichweite (neu)
- One-Stop-Shop (neu)
- Regelungen zur Auftragsverarbeitung (erweitert)

Details im Anhang

WAS IST UNVERÄNDERT / WAS IST NEU?

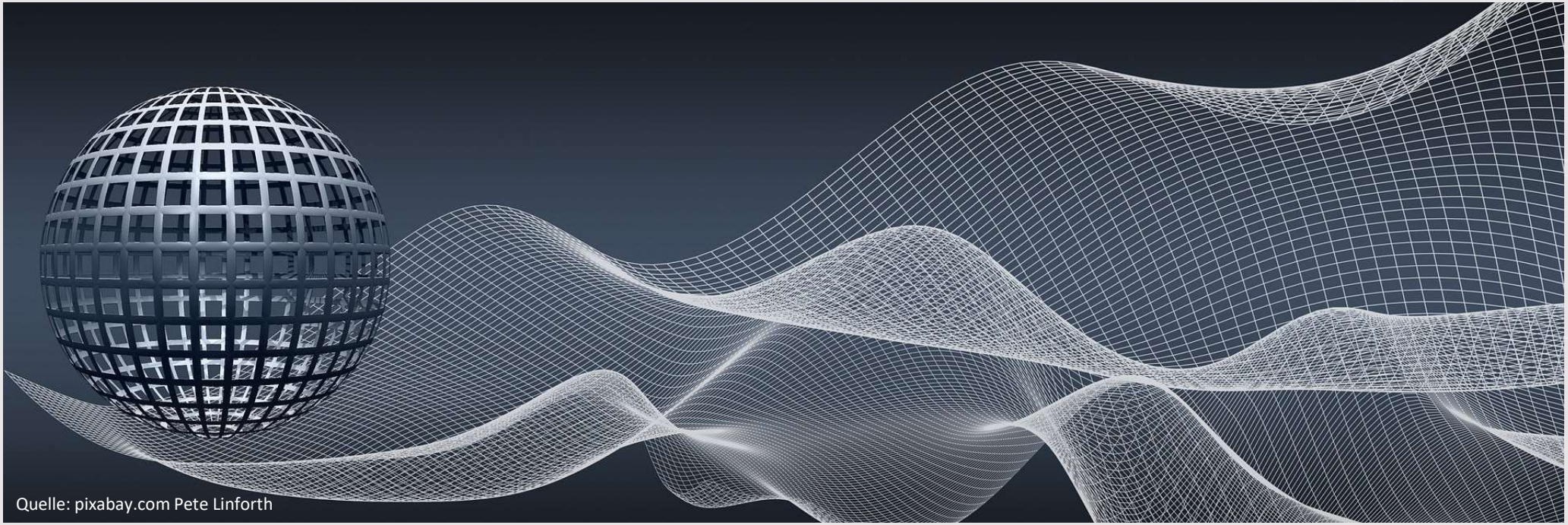
- Informationspflichten (neu)
- Grundsätze der Verarbeitung
  - Rechtmäßigkeit (erweitert um Treu und Glauben / Transparenz)
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung/Löschen
  - Integrität und Vertraulichkeit (erweitert)

WAS IST UNVERÄNDERT / WAS IST NEU?

- Risiko in Bezug auf Verarbeitung (neu)
- Rechenschaftspflicht (neu)
- Verarbeitungsverzeichnis (erweitert)
- Betroffenenrechte (deutlich erweitert)
- Meldepflichten bei Datenpannen (erweitert)
- Bußgelder (deutlich erweitert)
- Umfang besonderer Datenkategorien (erweitert)

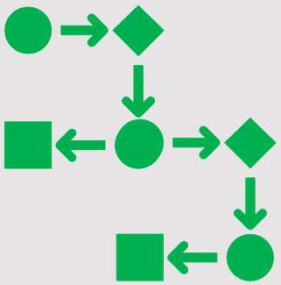
WAS IST UNVERÄNDERT / WAS IST NEU?

- Datenschutz durch Technikgestaltung (Neu)
  - Privacy by Design
- Datenschutz durch datenschutzfreundliche Voreinstellungen (Neu)
  - Privacy by Default
- Datenschutz-Folgeabschätzung (Neu?)


Quelle: pixabay.com Pete Linforth

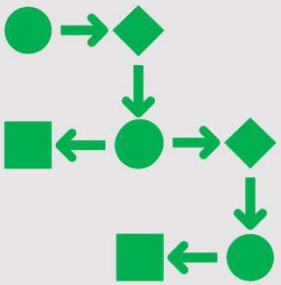
Privacy by Design und Privacy by Default

PRIVACY BY DESIGN AND DEFAULT



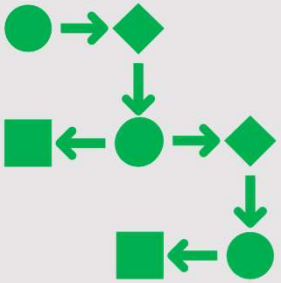
- Privacy by Design and Default kürzer als „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“
- vs „DS von der Entwurfsphase an (FR)“ vs „DS beim Entwurf (ES)“ vs „DS ab der Konzeption (PT)“
- Ziel ist es, die Gestaltung von Systemen und Diensten derart, das die Datenschutzgrundsätze frühzeitig beachtet werden und möglichst viele datenschutzfreundliche Voreinstellungen vorliegen.
- Historisch basierend auf der Datenvermeidung und Datensparsamkeit des deutschen BDSG a.F.

DSGVO ART. 25 (1)



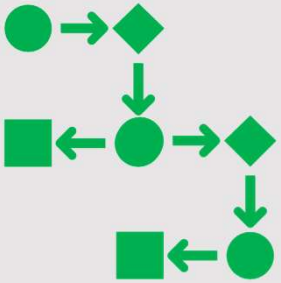
- Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen
- trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung
- geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

DSGVO ART. 25 (1)



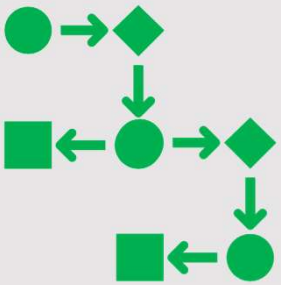
- Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen
- trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung
- geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

GRUNDSÄTZE DER VERARBEITUNG



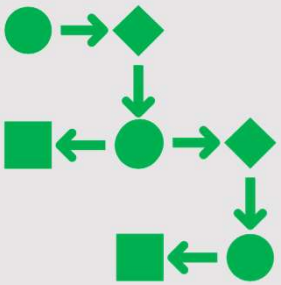
- Rechtmäßigkeit (erweitert um Treu und Glauben / Transparenz)
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung/Löschen
- Integrität und Vertraulichkeit (erweitert)

DSGVO ART. 25 (2)



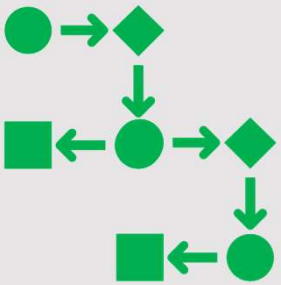
- Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.
- Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

DSGVO ERWÄGUNGSGRUND (78)



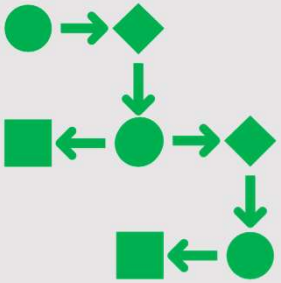
- Solche Maßnahmen (.. die insbesondere den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen Genüge tun ..) könnten unter anderem darin bestehen,
  - dass die Verarbeitung personenbezogener Daten minimiert wird,
  - personenbezogene Daten so schnell wie möglich pseudonymisiert werden,
  - Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird,
    ….

DSGVO ERWÄGUNGSGRUND (78)

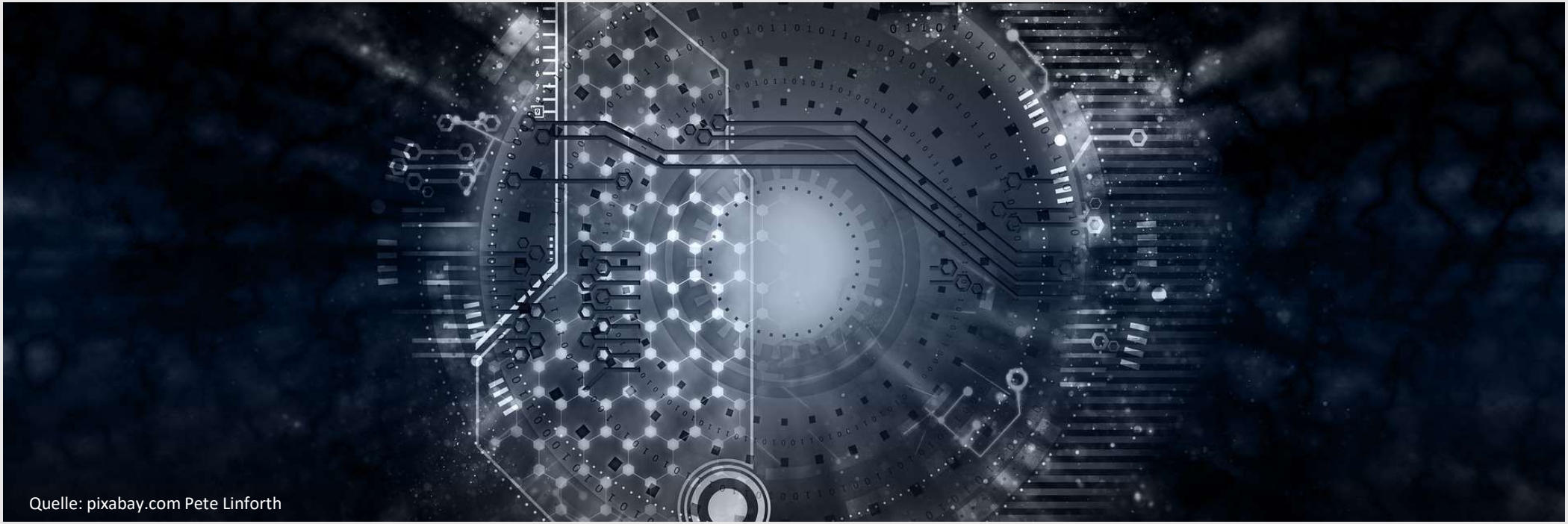


- Solche Maßnahmen (.. die insbesondere den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen Genüge tun ..) könnten unter anderem darin bestehen,
  - …
  - der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und
  - der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern.
- Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.

MASSNAHMEN



- Aggregation / Pseudonymisierung / Anonymisierung
- Kurze Speicherfristen / automatisiertes Löschen am Zweckende (ggf. auf Feldebene) / Löschkonzept
- Feldgenaue Dokumentation der Zwecke
- Transparenz durch Information und Prozesse zu Betroffenenrechten
- Symbolkennzeichnung / Maschinenlesbare Datenschutzerklärungen
- Werkzeuge zur Selbstauskunft / Datenverarbeitung-Brief



Quelle: pixabay.com Pete Linforth

Datenschutz-Folgeabschätzung (DSFA)

DATENSCHUTZ-FOLGE-ABSCHÄTZUNG (DSFA)

- Data Protection Impact Assessment (DPIA)
- Verbindet Recht und Sicherheit
- Ist geeignet, um hohe Risiken für den Betroffenen zu identifizieren, zu bewerten und Abhilfe zu schaffen.
- Ursprünge vor DSGVO (Ziel: Transparenz)
  - Privacy Impact Assessment in UK, CAN seit 90er
  - Vorabprüfung in EU DS-Richtlinie von 1995
  - Vorabkontrolle in BDSG a.F.

DSGVO ART. 35 (1)

- Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

DSGVO ART. 35 (1) - DETAILS

- Voraussichtlich: eine frühe Abschätzung ist bereits bei der Planung durchzuführen
- hohes Risiko: Risikobegriff nicht definiert, aber herleitbar, Schäden können dabei physischer, materieller und immaterieller Natur sein
- Rechte und Freiheiten natürlicher Personen: Formulierung geht über Datenschutz hinaus und betrifft alle Grundrechte gemäß EU-Grundrechte-Charta und Menschenrechts-Konvention
- Vorab: die DSFA ist auf jeden Fall vor einer Verarbeitung durchzuführen

DATENSCHUTZ-FOLGE-ABSCHÄTZUNG (DSFA)

- Es genügt, wenn ein Teil der Verarbeitung ein hohes Risiko für den Einzelnen aufweist,
- Es handelt sich nicht um ein Unternehmensrisiko wie im herkömmlichen Risikomanagement.
- Durch den Verantwortlichen durchzuführen, regelmäßig nicht durch den Datenschutz-Beauftragten. Der DSB
  - berät den Verantwortlichen, ob DFSA notwendig
  - unterstützt bei Methodik
  - prüft, ob Maßnahmen der Risikominderung dienen und die Korrektheit der DSFA.

DATENSCHUTZ-FOLGE-ABSCHÄTZUNG (DSFA)

- Hersteller/IT-Dienstleister sind keine Verantwortlichen und müssen daher keine DFSA für Produkt durchführen.
- Generische DFSA zur Stärkung des DS und des Angebots, da der Hersteller das umfassendste Verständnis der technischen Eigenschaften hat.
- Bei Auftragsverarbeitung (z.B. Cloudservice) hat der Auftragnehmer eine gemeinsame Verantwortung und muss bei DFSA unterstützen.
- Im AV-Vertrag sollten daher festgelegt werden, wer für welche Schutzmaßnahmen zur Risikominderung zuständig ist.

WANN BENÖTIGT MAN EINE DSFA?

- Entscheidung ob DSFA durchgeführt werden muss:
  - gemäß DSGVO Art 35 (1) „Verwendung neuer Technologien“ und in (3) beschriebene Sachverhalten
  - Listen des EDSA/Art 29-Gruppe (9 Kriterien)
  - Leitlinie der Datenschutz-Konferenz (17 Kriterien)
  - Eigenständige Prüfung

DSGVO ART. 35 (7) – INHALT DER DSFA

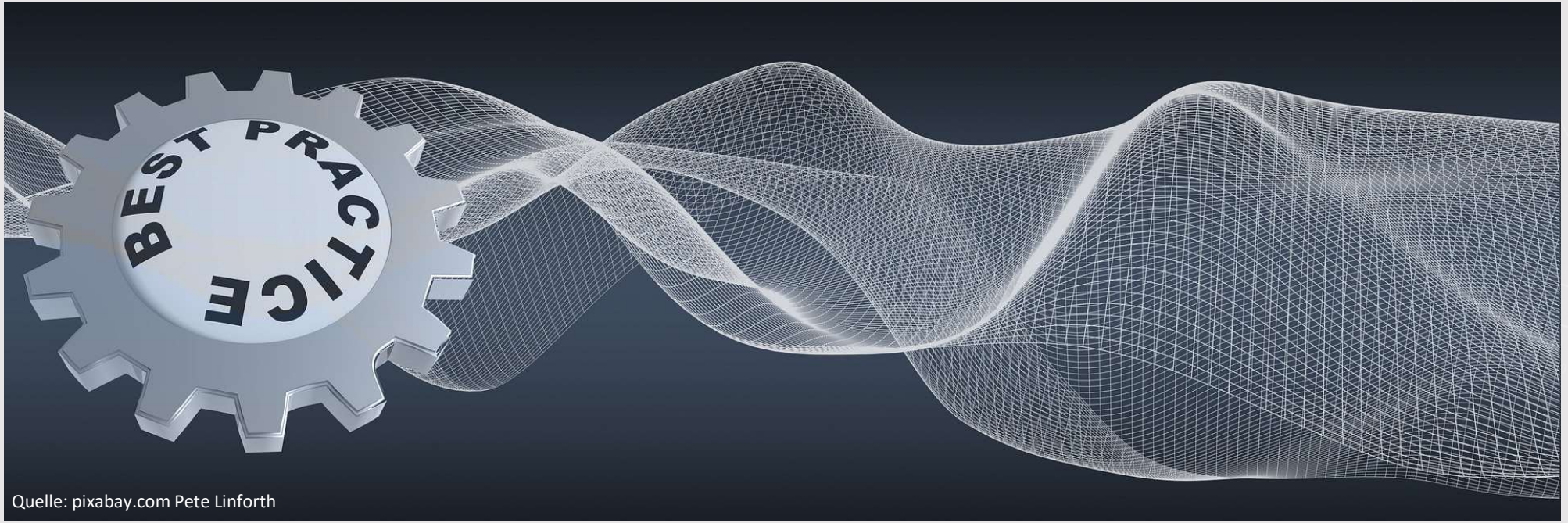
- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, …
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, … wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

DATENSCHUTZ-FOLGE-ABSCHÄTZUNG (DSFA)

- Die Betroffenen sollen gegebenenfalls befragt werden.
- Die Ergebnisse der DSFA sind zu dokumentieren.
  - Positives Ergebnis, d.h. Risiken sind ausreichend reduziert: Beginn der Verarbeitung möglich
  - Negatives Ergebnis: keine Verarbeitung oder Konsultation mit Aufsichtsbehörde
- Die DSFA ist regelmäßig zu wiederholen, insbesondere bei Änderung der Risiken.

BEISPIEL EINER DSFA

- Datenschutz-Folgenabschätzung (DSFA) für die deutsche Corona-App (Juni 2020)
  - https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf
- Datenschutz-Folgenabschätzung (DSFA) als Anlage zum Gesetzentwurf „Gesetz zur digitalen Modernisierung von Versorgung und Pflege (DVPMG)“(Dez 2020)
  - https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/guv-19-lp/dvpmg.html



Quelle: pixabay.com Pete Linforth

Fazit

KEY POINTS

- Datenschutz bereits im Pflichtenheft beachten
- Prozesse zur Softwareentwicklung anpassen
  - Dokumentation und Schulung für Entwickler
  - ErwGr 78 beachten
- Standardeinstellungen prüfen
- Prozess zur Datenschutz-Folgeabschätzung einführen
  - DSFA regelmäßig wiederholen
  - DSB einbeziehen

Michael Morgenthaler

CDPSE, CISA, CISM, FIP, CIPT, CIPP/E, DS-Auditor (TÜV)

morgenthaler@dsb-mm.de

www.dsb-mm.de

Quelle: pixabay.com Gerd Altmann

Quelle: pixabay.com Pete Linforth

Weitere Informationen

„PERSONENBEZOGENE DATEN“

- [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann; …

ERLAUBNISVORBEHALT I

Artikel 6 DSGVO Rechtmäßigkeit der Verarbeitung

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

ERLAUBNISVORBEHALT II

- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt; (gekürzt)
- Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich. (gekürzt)

Grundsätze der Verarbeitung personenbezogener Daten I

Artikel 5 DSGVO (1) Personenbezogene Daten müssen

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (Zweckbindung); (gekürzt)

Grundsätze der Verarbeitung personenbezogener Daten II

- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; („Speicherbegrenzung“); (gekürzt)

Grundsätze der Verarbeitung personenbezogener Daten III

- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);
- Artikel 5 DSGVO (2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

DSGVO ERWÄGUNGSGRUND (78)

- Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.

Artikel 35 DSGVO DSFA-Kriterienliste

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

- a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
- b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
- c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

DSFA Kriterienliste des Eur. Datenschutzausschusses

- Evaluierung oder Scoring, inklusive Profilbildung und Vorhersagen
- Automatisierte Entscheidungen mit rechtlicher/ ähnlich beeinträchtigender Wirkung
- Systematische Beobachtung
- Sensible Daten
- In großem Umfang verarbeitete Daten
- Datensätze, die abgeglichen oder kombiniert wurden
- Daten, die verletzliche Datensubjekte betreffen
- Innovative Nutzung/Verwendung von technologischen und organisat. Lösungen
- Fälle, in denen die Verarbeitung an sich „die betroffenen Personen an der Ausübung eines Rechts … hindert“
- https://www.datenschutz-bayern.de/technik/orient/wp248.pdf
- https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_de

DSFA Kriterienliste der Datenschutzkonferenz der Länder

- 17 Kriterien wobei…
  - Diese Liste ist nicht abschließend, sondern ergänzt die in den Absätzen 1 und 3 des Artikels 35 DSGVO enthaltenen allgemeinen Regelungen.
  - Diese Liste orientiert sich an der allgemeinen, im Arbeitspapier 248 Rev. 1 Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ beschriebenen Vorgehensweise. Sie ergänzt und konkretisiert diese allgemeine Vorgehensweise.
- https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf

LITERATUR

- https://www.fiff.de/dsfa-corona
- https://www.bitkom.org/sites/default/files/pdf/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf
- https://www.datenschutz-bayern.de/technik/orient/wp248.pdf
- https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf
- https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_de