Datenschutzwissen.de

Information - Seminare - Schulung - Workshops - Beratung

Die EU-Datenschutz-grundverordnung und ihre Folgen für Universitäten und Hochschulen

Diplom-Informatiker Werner Hülsmann
- Datenschutzsachverständiger -
Münchener Str. 101 / Geb. 01 • D-85737 Ismaning
E-Mail: wh@datenschutzwissen.de
https://dsgvo.expert

Platz für Notizen:

Zu meiner Person

1982 – 1988	Studium der Informatik an der TU Darmstadt Schwerpunkt Datenschutzrecht
1988 – 1991	Softwareentwickler bei der Telenorma GmbH, Frankfurt (Main)
1992 – 1999	Wissenschaftlicher Mitarbeiter und Referatsleiter Technik beim Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen
1999 – 2001	Datenschutz- und Technologieberatung bei ForBIT e.V. in Hamburg
Seit 1999	selbständiger Datenschutzberater (Datenschutzconsulting.eu)
2001 - 2002	Projektmanager Dataprotection bei der Telegate AG (Martinsried)
2003 - 2009 und seit 2014	Mitglied im Vorstand der Deutschen Vereinigung für Datenschutz (DVD) e.V., Bonn - www.datenschutzverein.de
2004 - 2015	Kooperationspartner des virtuellen Datenschutzbüros
2004	Gründung von Datenschutzwissen.de – Organisation und Leitung von Datenschutzseminaren
Seit 2004	beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich/technisch)
Seit 2010	Expert for legal and technical evaluations for the European Privacy Seal (EuroPriSe, http://www.european-privacy-seal.eu/)

Wichtige Hinweise

- Diese Unterlagen sind auf dem Stand vom 30.06.2017
  - Die Darstellung der „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“ (DSGVO) basiert auf der im EU-Amtsblatt veröffentlichten Fassung der DSGVO unter Berücksichtigung des Corrigiums vom November 2016 (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72).
    - Ergänzend wurden einige redaktionelle und Übersetzungsfehler vom Autor korrigiert.
  - Die Darstellung des ab dem 25. Mai 2018 geltenden neuen Bundesdaten-schutzgesetz (BDSG-neu) basiert auf dem Beschluss des Dt. Bundestages vom 27. April 2017 zur BT-Drs. 18/11325 (Gesetzentwurf) in der Fassung der BT-Drs. 18/12084 (Beschlussempfehlung des Innenausschusses)
    - Hier wurden ebenfalls redaktionelle Fehler vom Autor korrigiert
- Der Inhalt dieser Unterlagen wurden mit größter Gewissenhaftigkeit und aller Sorgfalt zusammengestellt. Dennoch kann der Autor keine Gewähr für Fehlerfreiheit übernehmen.

Platz für Notizen:

Gliederung 1/2

- Überblick über die DSGVO
  - Ziele und wesentliche Inhalte der DSGVO
  - Stellung des behördlichen Datenschutzbeauftragten nach Gültigwerden der DSGVO
  - Beschäftigtendatenschutz in der DSGVO
    - Auswirkung auf vorhandenen Dienstvereinbarungen
  - Verarbeitung personenbezogener Daten für Zwecke der Forschung und Wissenschaft nach der DSGVO
- Die Rechte des Betroffenen (u.a., Portabilität; Informations- und Auskunftsrechte; das Recht auf Vergessenwerden)

Gliederung 2/2

- Datenschutz durch Technik?!
- Handlungs- und Regelungsbedarf in Hochschulen und Universitäten
  - Vom Verfahrensverzeichnis zum Verzeichnis von Verarbeitungstätigkeiten
  - Auftragsdatenverarbeitung: Was ändert sich gegenüber § 11 DSG NRW?
- Weitere aktuelle Entwicklungen

Platz für Notizen:

Datenschutz?

- Datenschutz schützt nicht die Daten, sondern dient dem Schutz der Privatspähre sowie der Grundrechte und Grundfreiheiten der betroffenen Personen.
- Datenschutz ist keine moderne Erfindung, sondern gibt es bereits seit der Antike (z.B. im Hippokratischen Eid).
- Datenschutz ist ein Menschenrecht.
- Der Datenschutz – das Recht auf informationelle Selbstbestimmung – wurde 1983 vom BVerfG aus den Grundrechten der Art. 1 und 2 des Grundgesetzes abgeleitet.
- Datenschutz ist seit 2009 auch in der Europäischen Grundrechtecharta verankert.

Datenschutzentwicklung in Deutschland und der EU

- 1971: Hessisches Landesdatenschutzgesetz
- 1977: Erstes Bundesdatenschutzgesetz
- 1980: OECD: Leitlinien für den Schutz des Persönlichkeits-bereichs und den grenzüberschreitenden Verkehrs personenbezogener Daten
- 1981: Europarat: Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten
- 1983: Volkszählungsurteil des BVerfG: Recht auf Informationelle Selbstbestimmung
- 1995: EG-Datenschutz-Richtlinie 95/46/EG (umzusetzen bis Oktober 1998, in D 2001 umgesetzt)
- 2009: Europäischen Grundrechtecharta
- 2016: EU-Datenschutzgrundverordnung

Platz für Notizen:

Überblick über die DSGVO

Werden und Status der DSGVO

- Im Januar 2012 hat die Europäische Kommission ein umfassendes Paket zur Neuregelung des Datenschutzes in Europa vorgestellt
- Ein Teil diese Pakets war der Vorschlag für die DSGVO, die mit ihrem Wirksamwerden die bisherige Richtlinie ersetzen wird.
- Die Endfassung wurde am 08. April vom Ministerrat und am 14. April 2016 vom EU-Parlament verabschiedet.
- Sie wurde am 04. Mai 2016 im EU-Amtsblatt veröffentlicht.
- Die Verordnung tritt „am 20. Tag nach der Veröffentlichung im Amtsblatt der Europäischen Union in Kraft“ (Art. 99 Abs. 1), als am 25. Mai 2016.
- Gültig wird die Verordnung zwei Jahre nach ihrem Inkrafttreten (Art. 99 Abs. 2) und damit am 25. Mai 2018
- „Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.“ (Satz nach Art. 99)

Platz für Notizen:

Die Europäische Datenschutzgrundverordnung – Ziele und wesentliche Inhalte der DSGVO

Folie 11

Verordnung statt Richtlinie

- Derzeit gilt für den Datenschutz auf EU-Ebene insbesondere die sogenannte Datenschutzrichtlinie von 1995 (in ihrer aktuellen Fassung)
- Diese Richtlinie war von den Mitgliedstaaten der EU in nationales Recht umzusetzen. Dies wurde auf teilweise sehr unterschiedliche Weise erledigt und ist in Deutschland im BDSG, den LDSGen und bereichsspezifischen Regelungen erfolgt.
- Ein wesentliches Ziel, dass mit der DSGVO erreicht werden soll, ist die Schaffung EU-weit einheitlicher Regelungen zum Datenschutz
- Die Verordnung gilt ab ihrem Gültigwerden am 25. Mai 2018 direkt! Einer Umsetzung in nationales Recht bedarf es daher nicht mehr!
- Nationalen Datenschutzrechts ist allerdings anzupassen.
- Erforderlich ist die Verabschiedung von Regelungen zur Nutzung der sogenannten „Öffnungsklauseln“ mit denen die Mitgliedstaaten die Möglichkeit erhalten, bisherige Regelungen (wie z.B. zum betrieblichen Datenschutz-beauftragten und im Gesundheitsdatenschutz) beizubehalten oder neue solche Regelungen einzuführen.

Datenschutzwissen.de
Information · Seminare · Schulung · Workshops · Beratung

Platz für Notizen:

Folie 12

Erwägungsgründe und Artikel

- Der eigentlichen Regelungen des Verordnungstextes finden sich in den 99 Artikeln der DSGVO.
- Davor finden sich 172 sogenannten Erwägungsgründe.
- Diese Erwägungsgründe stellen zwar selbst keine rechtlichen Regelungen dar, sondern beinhalten die Motive zur und Gründe für die Einführung der entsprechenden Artikel.
- Die Erwägungsgründe helfen bei der Auslegung der Regelungen der Artikel.
- Viele Erwägungsgründe beziehen sich dabei auf konkrete Artikel
- **Hinweis:** Oft ist es für das Verständnis hilfreich, die englische Originalfassung hinzuzunehmen, da es in der deutschen Fassung Übersetzungsungenauigkeiten und redaktionelle Fehler gibt.

Datenschutzwissen.de
Information · Seminare · Schulung · Workshops · Beratung

Platz für Notizen:

Die Europäische Datenschutzgrundverordnung – Wichtige Regelungen

Wesentliche Änderungen durch die DSGVO

- Die Betroffenenrechte werden deutlich ausgeweitet.
- Die Dokumentationspflichten werden deutlich ausgeweitet.
- Es gibt viele neue Bußgeldtatbestände.
- Die Bußgelder werden drastisch erhöht.
- Die Anforderungen an den technischen Datenschutz erhöhen sich.
- Privacy by Design und Privacy by Default (Stichwort: Datenminimierung) werden Pflicht.
- Eine Risikoabschätzung für Datenverarbeitungen wird zur Regel.

Was bleibt?

- Viele bereits seit langem bekannte Regelungsinhalte bleiben erhalten.
- Vor allem bleibt es im Datenschutzrecht beim „Verbot mit Erlaubnisvorbehalt“
- Es gibt – auch auf EU-Ebene – weiterhin bereichsspezifische Regelungen, wie z.B.
  - die EU-Datenschutzrichtlinie für die elektronische Kommunikation (Richtlinie 2002/58/EG, „Cookie-Richtlinie“), die derzeit überarbeitet wird oder
  - die EU-Datenschutzrichtlinie für Polizei und Justiz („Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates“), vgl. http://eur-lex.europa.eu/procedure/DE/201285

Platz für Notizen:

Was bleibt?

- Behörden dürfen Daten nur zur Erfüllung ihrer Aufgaben verarbeiten, siehe Art. 6 DSGVO:

  „(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

  (...)

  f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

  Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.“

Folie 17

„Berechtigte Interessen“ als Erlaubnistatbestand?

- Für Behörden ist die Interessenabwägung als Erlaubnistatbestand in der DSGVO ausdrücklich ausgeschlossen.
- Auch bei anderen öffentlichen Stellen (die nicht als Behörde im Sinne der DSGVO gelten) ist davon auszugehen, dass berechtigte Interessen dieser Stellen (wie z.B. Hochschulen oder Unis) nur im Rahmen der gesetzlich vorgesehen Aufgaben liegen können.

Datenschutzwissen.de
Information · Seminare · Schulung · Workshops · Beratung

Platz für Notizen:

Folie 18

Was ändert sich?

- Die Höhe der möglichen Bußgelder (Art. 83 ff)
  - „Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und **abschreckend** ist.“ (Art. 83, Abs.1)
- Die Datenschutzaufsicht (Kapitel VI und VII, Art. 51 ff)
  - Deutschland hat nur eine Stimme im Europäischen Datenschutzausschuss.
  - Die Datenschutzaufsichts-Behörden in der EU und dem EWR sind verpflichtet die DSGVO einheitlich auszulegen, hierzu sind entsprechende Verfahren zur Abstimmung erforderlich
  - An der Zuständigkeit der/des LfDI NRW für die Hochschulen und Universitäten ändert dies allerdings nichts.

Datenschutzwissen.de
Information · Seminare · Schulung · Workshops · Beratung

Was fällt weg?

- Eine Verpflichtung auf das Datengeheimnis (§ 6 DSG NRW) findet sich in der DSGVO nicht (direkt).
- Spezielle Regelungen für Videoüberwachung und Videoaufzeichnung (§ 29b DSG NRW)
- Spezielle Regelungen zu mobilen personenbezogenen Speicher- und Verarbeitungsmedien (§ 29a DSG NRW)
- Das „Jedermannsrecht“ (§ 8 (2) DSG NRW) in Bezug auf die öffentlichen Verfahrensbeschreibungen.

Platz für Notizen:

Was ist neu?

- Meldepflicht von Datenschutzverletzungen an die Aufsichtsbehörde und Benachrichtigung der Betroffenen (Art. 33 und 34)
  - Diese gab es auf Bundesebene bereits
- Die Möglichkeit verbindliche Verhaltensregeln zu erstellen und von der zuständigen Aufsichtsbehörde genehmigen zu lassen (Art. 40).
  - Dies gab es auf Bundesebene bereits.

Die behördlichen Datenschutzbeauftragten

- Nach Art. 37 DSGVO haben alle öffentlichen Stellen eine/n Datenschutzbeauftragte/n zu benennen.
- Die DSGVO kennt im Gegensatz zum DSG NRW keine StellvertreterInnen des/der behördlichen Datenschutzbeauftragten
- Es steht den Behörden aber frei, mehr als eine/n Datenschutzbeauftragte/n und/oder einen oder mehrere StellvertreterInnen zu benennen.
- Die Stellung der behördlichen Datenschutzbeauftragten ist in Art. 38 DSGVO geregelt.
- Die Aufgaben der behördlichen Datenschutzbeauftragten sind im Art. 39 DSGVO aufgeführt.

Platz für Notizen:

Stellung der behördlichen Datenschutzbeauftragten

- Die Stellung der behördlichen Datenschutzbeauftragten ist in Art. 38 DSGVO geregelt.
- An der Stellung der behördlichen Datenschutzbeauftragten ändert sich im Grunde nichts (vgl. Art. 38 Abs. 3):
  - Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält.
  - Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden.
  - Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters.

Folie 23

Aufgaben der behördlichen Datenschutzbeauftragten

- Die Aufgaben der behördlichen Datenschutzbeauftragten sind in Art. 39 Abs. 1 DSGVO aufgeführt.
- Aufgrund dieser Aufgabenbeschreibung wird in der Fachliteratur diskutiert, ob die Datenschutzbeauftragten nach der DSGVO eine höhere Verantwortung tragen als die bisherigen Datenschutzbeauftragten nach BDSG.
- Die Aufgabenbeschreibung des § 32a DSG NRW ähnelt allerdings der Aufgabenbeschreibung aus der DSGVO:
  - „Der Beauftragte (...) hat die Einhaltung der datenschutzrechtlichen Vorschriften zu überwachen, die mit der Verarbeitung personenbezogener Daten befassten Personen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen“
- Gegenüber der Verantwortung, die sich bereits jetzt aus § 32a DSG NRW ergibt, ist daher vermutlich keine Erhöhung der Verantwortung durch die DSGVO zu sehen.

Datenschutzwissen.de
Information · Seminare · Schulung · Workshops · Beratung

Platz für Notizen:

Folie 24

Beschäftigtendatenschutz in der DSGVO

- Die DSGVO enthält selbst (fast) keine Regelungen zum Beschäftigtendatenschutz.
  - Im Erwägungsgrund 48 wird die Übermittlung von Beschäftigtendaten „innerhalb der Unternehmensgruppe für interne Verwaltungszwecke“ ausdrücklich als mögliches berechtigtes Interesse aufgeführt.
  - In Art. 9 Abs.2 Buchstabe h wird die Verarbeitung von besonderen Datenarten, zu denen u.a. die Gesundheitsdaten gehören, zu Zwecken „der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten“ ausdrücklich erlaubt.
- Nach Art. 88 DSGVO dürfen „Mitgliedstaaten durch Rechtsvorschriften und Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext (…) vorsehen.“
  - Dienstvereinbarungen als Regelungen zum Umgang mit Beschäftigtendaten sind also weiterhin möglich.

Datenschutzwissen.de
Information · Seminare · Schulung · Workshops · Beratung

Beschäftigtendatenschutz in der DSGVO

- Art. 88 Abs. 2 fordert von solchen Regelungen:
- „Diese Vorschriften umfassen angemessene und besondere Maßnahmen zur Wahrung
  - der menschlichen Würde,
  - der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf
    - die Transparenz der Verarbeitung,
    - die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und
    - die Überwachungssysteme am Arbeitsplatz.“

Platz für Notizen:

Auswirkung auf vorhandene Dienstvereinbarungen?

- Sofern die Dienstvereinbarungen, in denen die Verarbeitung von Beschäftigtendaten geregelt sind, den Anforderungen aus Art. 88 DSGOV genügen, sind keine Änderungen erforderlich.
- „Diese Vorschriften umfassen angemessene und besondere Maßnahmen zur Wahrung
  - der menschlichen Würde,
  - der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf
    - die Transparenz der Verarbeitung,
    - die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und
    - die Überwachungssysteme am Arbeitsplatz.“
- Bestehende Dienstvereinbarungen sind daher daraufhin zu überprüfen, ob diese Anforderungen erfüllt sind.

Verarbeitung pbD in Forschung & Wissenschaft nach d. DSGVO

- Art. 89 Abs. 1 DSGVO sagt aus:
  - „Die Verarbeitung (...) zu wissenschaftlichen oder historischen Forschungszwecken (...) unterliegt geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung."
  - „Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird."
- Zu diesen Maßnahmen gehört die Pseudonymisierung, wenn eine solche den Zweck der Verarbeitung nicht gefährdet.

Platz für Notizen:

Verarbeitung pbD in Forschung & Wissenschaft nach d. DSGVO

- Nach § 28 Abs. 1 DSG NRW soll die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken in anonymisierter Form erfolgen.
- Eine Verarbeitung in pseudonymisierter Form ist nur zulässig, wenn der Anoynymisierung wissenschaftliche Gründe entgegen stehen und wenn sichergestellt ist, dass eine Depseudonymisierung den forschenden Personen nicht möglich ist.
- Ist weder eine Anonymisierung noch eine Pseudonymisierung möglich, ist die Verarbeitung nach § 28 Abs. 2 DSG NRW nur unter strengen Grenzen möglich.
- Die Daten sind so früh wie möglich zu anonymisieren oder pseudonymisieren.

=> Die Formulierungen der DSGVO sind wesentlich weicher als die des DSG NRW.

Verarbeitung anonymisierter Daten nach der DSGVO

- Aus Erwägungsgrund 26 DSGVO:
- Keine Anwendung der DSGVO für anonyme Daten:
  „Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.“
- Identifizierbare Person?
  „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.“

Platz für Notizen:

Verarbeitung anonymisierter Daten nach der DSGVO

- Ab wann Daten nicht mehr als anonym gelten hängt sehr stark ab von
  - dem jeweiligen Kontext,
  - den technischen Möglichkeiten und
  - dem potentiellen Interesse des Verantwortlichen oder eines Dritten anonymisierte Daten zu reanonymisieren.
- Es reicht also nicht aus, nur Namen, Anschrift und Geburtsdatum wegzulassen.
- Vielmehr ist unter Berücksichtigung des konkreten Datenbestandes zu prüfen, ab welcher Gruppengröße von einer echten Anonymisierung auszugehen ist.

Platz für Notizen:

Die Rechte der Betroffenen

Artikel 12 - Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

- Art. 12 DSGVO regelt, wie die Informationen der Art. 13 und 14 und die Mitteilungen der Art. 15 bis 22 und 34 zu gestalten sind:
- Sie sind "in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" zu übermitteln.
- „Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch."
- „Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde."
- Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung.
  - Diese Frist kann einmalig um zwei Monate unter bestimmten Bedingungen verlängert werden. Der Betroffene ist hierüber spätestens zum Ablauf der ursprünglichen Frist mit Angabe zu den Gründen zu informieren.

Artikel 13 und 14 - Informationspflichten

- Die Informationspflichten werden – unabhängig davon ob die Daten bei der betroffenen Person erhoben oder von Dritten erhalten werden – deutlich ausgeweitet.
- Es ist über insgesamt 12 Punkte zu informieren. Hierzu gehören
  - Kontaktdaten des/der Datenschutzbeauftragten
  - Zwecke der Verarbeitung
  - berechtigte Interessen, falls diese als Rechtsgrundlage dienen sollen
  - beabsichtigte Datenübermittlungen an ein Drittland
  - Recht auf Widerruf der Einwilligung, Recht auf Berichtigung, Löschung, oder auf Einschränkung der Verarbeitung, Recht auf Widerspruch, Recht auf Datenübertragbarkeit
  - Recht sich bei der Aufsichtsbehörde zu beschweren
  - Ist die Bereitstellung der Daten vertraglich oder gesetzlich vorgeschrieben oder zum Vertragsabschluss erforderlich?
  - Informationen zu automatisierten Einzelfallentscheidungen und zum Profiling
  - Informationen über Zweckänderungen

Platz für Notizen:

Artikel 15 - Auskunftsrecht der betroffenen Person

- Die betroffene Person hat ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:
  - die Informationen, die in der Informationspflicht enthalten sind
  - eine Kopie der gespeicherten Daten
- Wird der Antrag auf Auskunft elektronisch gestellt, sind die Informationen in einem „gängigen elektronischen Format“ zur Verfügung zu stellen, es sei denn die betroffene Person hat etwas anderes angegeben.
- Abs. 3 regelt, dass eine Kopie der Daten unentgeltlich bereitzustellen ist. Für weitere Kopien darf ein angemessenes Entgelt erhoben werden.

Artikel 16 - Recht auf Berichtigung

- Kurz und knapp ist hier geregelt:
  - Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.
  - Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.
- Unter Berücksichtigung des Grundsatzes der Richtigkeit aus Artikel 5 Buchstabe d) sollte es im eigenem Interesse des Verantwortlichen liegen, auch ohne Verlangen des Betroffenen für die Richtigkeit der Daten – soweit ihm das möglich ist – zu sorgen.

Platz für Notizen:

Artikel 17 - Recht auf Löschung („Recht auf Vergessenwerden“)

Gemäß Abs. 1 sind Daten auf Verlangen der betroffenen Person zu löschen, wenn:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

Artikel 17 - Recht auf Löschung („Recht auf Vergessenwerden“)

e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

- Hat der verantwortliche die Daten veröffentlicht und ist er zur Löschung verpflichtet, so hat er nach Abs. 2 angemessene Maßnahmen zu ergreifen, um andere Verantwortliche, die diese Daten verarbeiten darüber zu informieren, dass Links zu diese vormals veröffentlichten Daten und alle Kopien dieser Daten zu löschen sind.
- Abs. 3 regelt die Ausnahmen zu Abs. 1 und 2

Platz für Notizen:

Artikel 18 - Recht auf Einschränkung der Verarbeitung

- Die Einschränkung der Verarbeitung entspricht in etwa dem bisherigen Sperren von Daten.
- Die Verarbeitung personenbezogener Daten ist einzuschränken, wenn:
  - die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,
  - die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;
  - der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
  - die betroffene Person Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Artikel 18 - Recht auf Einschränkung der Verarbeitung

- In Erwägungsgrund 67 DSGVO sind Methoden zur Einschränkung der Verarbeitung ausdrücklich angegeben.
- „(2) Wurde die Verarbeitung gemäß Absatz 1 eingeschränkt, so dürfen diese personenbezogenen Daten — von ihrer Speicherung abgesehen — nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden.“
- (3) Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Absatz 1 erwirkt hat, wird von dem Verantwortlichen unterrichtet, bevor die Einschränkung aufgehoben wird.

Platz für Notizen:

Artikel 19 - Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

„Der Verantwortliche teilt allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Artikel 16, Artikel 17 Absatz 1 und Artikel 18 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.“

- Hieraus folgt, dass zu dokumentieren ist, welche Daten an welche Empfänger übertragen wurden und zwar so lange, wie diese Daten beim Verantwortlichen verarbeitet werden.
- Für die Umsetzung dieser Mitteilungspflicht und der Auskunft an die betroffene Person sollten entsprechende Prozesse eingeführt werden.
- Es ist zu dokumentieren, warum die Mitteilung unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden sein sollte.

Artikel 20 - Recht auf Datenübertragbarkeit

- (1) Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern
  - a) die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und
  - b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.
- Für alle Datenverarbeitungen, die auf anderer Rechtsgrundlage als Einwilligung oder Vertrag erfolgen, gilt dieses Recht nicht!

Platz für Notizen:

Artikel 20 - Recht auf Datenübertragbarkeit

- Absatz 2 sieht vor, dass die betroffene Person das Recht hat, dass die Daten direkt vom Verantwortlichen zu einem neuen Verantwortlichen übertragen werden, sofern dies technisch möglich ist.
- Das Recht auf Löschung („Recht auf Vergessenwerden“) bleibt hiervon unberührt. Insbesondere dürfen die Daten nicht nach der Übertragung gelöscht werden, wenn sie noch zur Vertragserfüllung benötigt werden.
- Das Recht auf Datenübertragbarkeit „gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.“
  - Welche Verarbeitungen dies sind, wird vom nationalen Gesetzgeber in bereichsspezifischen Gesetzen bestimmt.
- Die Rechte und Freiheiten anderer Personen dürfen durch die Wahrnehmung dieses Rechts nicht beeinträchtigt werden.

Artikel 21 - Widerspruchsrecht

„(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen."

„e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt."

Platz für Notizen:

Artikel 21 - Widerspruchsrecht

- Hier ist der Erwägungsgrund 69 erläuternd:

„Dürfen die personenbezogenen Daten möglicherweise rechtmäßig verarbeitet werden, weil die Verarbeitung für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt — die dem Verantwortlichen übertragen wurde, — oder aufgrund des berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist, sollte jede betroffene Person trotzdem das Recht haben, Widerspruch gegen die Verarbeitung der sich aus ihrer besonderen Situation ergebenden personenbezogenen Daten einzulegen. Der für die Verarbeitung Verantwortliche sollte darlegen müssen, dass seine zwingenden berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben."

- Gerade im öffentlichen Bereich dürfte die Anwendung dieser Vorschrift gewisse Komplikationen mit sich bringen.
- Wichtig ist für die Verantwortlichen im öffentlichen Bereich, dass der Gesetzgeber im Gesetzgebungsverfahren überzeugen dargelegt hat, wieso bestimmte Datenverarbeitungen im öffentlichen Interesse zwingend erforderlich sind!

Artikel 21 - Widerspruchsrecht

- Die Absätze 2 und 3 behandeln das Widerspruchsrecht gegen eine Datenverarbeitung zum Zwecke der Direktwerbung.
- Ein solcher Widerspruch gegen die Verarbeitung personenbezogender Daten zum Zwecke der Direktwerbung (inkl. einem etwaigen damit im Zusammenhang stehenden Profiling) steht der betroffenen Person zu und ist vom Verantwortlichen zu befolgen.
- Absatz 4 schreibt vor, dass die betroffene Person „spätestens zum Zeitpunkt der ersten Kommunikation mit ihr“ ausdrücklich auf dieses Widerspruchsrecht hingewiesen werden muss
  - „dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.“ - Umsetzung?
- Absatz 5 sieht vor, dass dieses Widerspruchsrecht auch mittels technischer Einstellungen (wie z.B. durch die Aktivierung der „Do not track“-Option im Browser) ausgeübt werden kann
- Absatz 6 regelt den Widerspruch gegen die Verarbeitung „personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Artikel 89 Absatz 1 erfolgt“

Platz für Notizen:

Artikel 22 - Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

- Hiervon gibt es Ausnahmen, wenn diese Entscheidung
  - für den Abschluss oder die Erfüllung eines Vertrags zwischen betroffener Person und Verantwortlichem erforderlich sit
  - auf Grund von anderen Rechtsvorschriften (EU- oder nationales Recht) zulässig ist
  - mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.
- Ein vollautomatisertes Verfahren zur StudienbewerberInnen-Auswahl wäre – wenn nicht das Land NRW entsprechende Rechtsvorschriften erlässt – unzulässig.

Artikel 34 - Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

(2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen.

Diese sind:

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Platz für Notizen:

Artikel 34 - Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;

b) der Verantwortliche durch nachfolgende (nach der Datenschutzverletzung erfolgte) Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;

c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

- Absatz 4 sieht vor, dass die Aufsichtsbehörde eine solche Information der betroffenen Personen verlangen kann oder per Beschluss feststellen kann, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

Platz für Notizen:

Datenschutz und Technik? Datenschutz durch Technik!

Privacy by Design Privacy by Default

- Erwägungsgrund 4 fordert:
  „Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen“
- Die englische „Originalfassung“ ist da allerdings noch deutlicher:
  „The processing of personal data should be **designed** to serve mankind.“

Privacy by Design
Privacy by Default

- Der Artikel 25 - „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ enthält die Anforderung, Datenschutz bereits durch Technikgestaltung und datenschutzfreundliche Voreinstellungen zu fördern.
- Bereits bei der Auswahl der Mittel aber auch zum Zeitpunkt der eigentlichen Verarbeitung sind die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, „um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen“

Platz für Notizen:

Privacy by Design
Privacy by Default

- Die Maßnahmen sollen dazu ausgelegt sein, „die Datenschutzgrundsätze wie Datenminimierung wirksam umzusetzen“
- Dadurch wird es noch wichtiger, dass die Datenschutz-beauftragten bereits bei der Planung und Beschaffung neuer Systeme sowie bei der Änderung bestehender Systeme frühzeitig einbezogen werden. um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen

Privacy by Design
Privacy by Default

- Bei der Umsetzung kann der Einsatz von mit Datenschutz-gütesiegeln oder Datenschutzzertifikaten versehenen Produkten helfen.
- Eine enge Zusammenarbeit zwischen Fachabteilung, IT-Abteilung, Datenschutzbeauftragten, IT- oder Informationssicherheitsbeauftragten und Personalrat ist grundsätzlich erforderlich.
- Zu Beginn einer Beschaffung ist zu klären,
  - zu welchem rechtlich zulässigen Zweck die Datenverarbeitung notwendig ist und
  - welche Daten für den vorgesehenen Zweck zwingend erforderlich sind
- Anhand dessen sind die Anforderungen an das System zu formulieren.

Platz für Notizen:

Art. 32 – Sicherheit der Verarbeitung

- „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 des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;“

Folie 55

Gewährleistungsziele

Quelle: https://www.datenschutzzentrum.de/artikel/1134-Anforderungen-an-die-Technik-Zur-Regulierung-des-technischen-Datenschutzes.html

Datenschutzwissen.de
Information · Seminare · Schulung · Workshops · Beratung

Platz für Notizen:

Folie 56

Datenschutz-Folgen-abschätzungen

- Die Regelungen zur Datenschutz-Folgenabschätzung (DS-FA) finden sich in Art. 35.
- Die DS-FA löst die Vorabkontrolle quasi ab.
- Allerdings ist die DS-FA vom Verantwortlichen selbst durchzuführen. Der/die Datenschutzbeauftragte berät nur noch.
- Bei der Entscheidung, für welche Verarbeitungsvorgänge eine DS-FA erforderlich ist, haben die Aufsichtsbehörden eine entscheidende Rolle:
  - Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese.
  - Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.
- Zur Durchführung der DS-FA verweise ich auf
  - das Whitepaper Datenschutz-Folgenabschätzung des Forum Privatheit und
  - das Standard-Datenschutzmodell der dt. Datenschutzaufsichtsbehörden

Datenschutzwissen.de
Information · Seminare · Schulung · Workshops · Beratung

Handlungs- und Regelungsbedarf in Hochschulen und Universitäten

Platz für Notizen:

Vom Verfahrensverzeichnis zum Verzeichnis von Verarbeitungstätigkeiten

- Die Verfahrensverzeichnisse sind an die Anforderungen der DSGVO anzupassen.
- Weiterführende Informationen finden sich u.a. auf https://www.lda.bayern.de/de/datenschutz_eu.html
  - „Die deutschen Aufsichtsbehörden haben bereits eine Arbeitsgruppe gegründet, die das Ziel verfolgt, eine Mustervorlage für solch ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO zu erarbeiten. Geplant ist, diese Mustervorlage dann bis ca. Mitte 2017 zu veröffentlichen."
  - Das Verzeichnis „wird (...) eine wesentliche Rolle spielen, um datenschutzrechtliche Vorgaben überhaupt einhalten zu können. Nur wer die eigenen Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um eine rechtmäßige Verarbeitung personenbezogener Daten sicherstellen zu können."

Folie 59

Definition von „Verfahren“ in der DSGVO?

- Bisher gab es in der Begründung zu Art. 18 der EG-Datenschutzrichtlinie 1995 eine „Definition“:
  - Ein "Verfahren ist ein Bündel von Verarbeitungen, die über eine vom Verantwortlichen definierte Zweckbestimmung verbunden sind".
- In der DSGVO heißt es nun in der Überschrift des Artikel 30:„Verzeichnis von **Verarbeitungstätigkeiten**“.
- Der Begriff der „Verarbeitungstätigkeit“ wird in der DSGVO oft verwendet, aber nicht definiert.
- Definiert ist in Art. 4 Ziff. 2 DSGVO nur der Begriff der „Verarbeitung“, im Sinne der DSGVO bezeichnet der Ausdruck
  - „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten 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, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Platz für Notizen:

Folie 60

Verzeichnis von Verarbeitungstätigkeiten - wozu?

- Das Verzeichnis von Verarbeitungstätigkeiten ist gemäß Erwägungsgrund 82 zu erstellen, damit die betreffenden Verarbeitungen „kontrolliert werden können“.
- Das Verzeichnis von Verarbeitungstätigkeiten kann auch zur grundlegenden Basis der Umsetzung der Dokumentationspflichten genutzt werden.
  - Hierzu sollten neben den in Art. 30 genannten Inhalten insbesondere die Informationen hinzugefügt werden, die für die jeweilige Verarbeitungstätigkeit relevant sind, z.B.
    - Wer ist die verantwortliche Fachabteilung
    - Ist eine Datenschutz-Folgenabschätzung (s.u.) erforderlich und wenn ja, wie lautet das Ergebnis, wenn nein, warum nicht?
- Der Detaillierungsgrad des Verzeichnisses von Verarbeitungstätigkeiten sollte daher dem bisherigen internen Verfahrensverzeichnis entsprechen.

Auftragsdatenverarbeitung: Was ändert sich gegenüber § 11 DSG NRW?

Platz für Notizen:

Auftragsdatenverarbeitung nach der DSGOV

- Auftraggeber und Auftragnehmer, die bereits die Anforderungen des § 11 DSG NRW „Verarbeitung personenbezogener Daten im Auftrag“ erfüllen sind auch in Hinblick auf die Anforderungen der DSGVO gut aufgestellt.
- Allerdings sind die ADV-Vereinbarungen an die Anforderungen an die DSGVO anzupassen:
  - § 11 DSG NRW verlangt hier nur:
    „Der Auftrag ist schriftlich zu erteilen, wobei erforderlichenfalls ergänzende Weisungen zu technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind.“

Folie 63

Auftragsdatenverarbeitung nach der DSGOV

- Art. 28 Abs. 2 DSGVO sieht vor, dass Subunternehmer nur mit schriftlicher Erlaubnis des Auftraggebers hinzugezogen werden dürfen.
- Art. 28 Abs. 3 DSGVO sieht vor, dass in der ADV-Vereinbarung schriftlich folgende Punkte geregelt sind:
  - Gegenstand und Dauer der Verarbeitung,
  - Art und Zweck der Verarbeitung,
  - die Art der personenbezogenen Daten,
  - die Kategorien betroffener Personen und
  - die Pflichten und Rechte des Verantwortlichen
- Hier sind auch weitere Anforderungen genannt, die durch die ADV-Vereinbarung sicher gestellt sein muss.

Datenschutzwissen.de
Information · Seminare · Schulung · Workshops · Beratung

Platz für Notizen:

Folie 64

Auftragsdatenverarbeitung nach der DSGOV

- Der Auftragsverarbeiter (wie der Auftragnehmer nach der DSGVO heißt) hat nach der DSGVO deutlich höhere Verantwortlichkeiten als nach dem DSG NRW (oder dem BDSG)
  - Eigenes Verzeichnis von Verarbeitungen des Auftragsverarbeiters für die Auftragstätigkeiten
  - Schadensersatzansprüche auch gegen den Auftragsverarbeiter
  - Viele Artikel der DSGVO enthalten auch Verpflichtungen für den Auftragsverarbeiter
  - Ein „Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt“ gilt „in Bezug auf diese Verarbeitung als Verantwortlicher“ (Abs. 10)

Datenschutzwissen.de
Information · Seminare · Schulung · Workshops · Beratung

Auftragsdatenverarbeitung nach der DSGOV

- Neue ADV-Vereinbarungen sollten bereits jetzt so abgeschlossen werden, dass sie den Anforderungen der DSGVO entsprechen.
- Alle bereits bestehenden ADV-Vereinbarungen sollten bis zum 25. Mai 2018 an die Anforderungen der DSGVO angepasst werden.
  - Evtl. kann hier auf die Herausgabe von Musterverträgen durch die DS-Aufsichtsbehörden gewartet werden (aber nicht zu lange!) sofern diese rechtzeitig zur Verfügung gestellt werden.
  - Es gibt von Verbänden bereits Muster.
- Beide Maßnahmen sind im Interesse der Auftraggeber (Verantwortliche) und der Auftragsverarbeiter.

Platz für Notizen:

Weitere aktuelle Entwicklungen

Aktivitäten des Gesetzgebers in NRW

- Derzeit ist noch kein Entwurf zur Anpassung des DSG NRW an die DSGVO bekannt.
- Die Landesgesetzgeber haben das Gesetzgebungsverfahren des Bundes abgewartet.
- Gerade für die Datenverarbeitung öffentlicher Stellen gibt es für die nationalen Gesetzgeber – und damit im Bereich der Länder – für die Landesgesetzgeber umfangreiche Konkretisierungs- und Regelungsklauseln in der DSGVO.
- Diese Regelungsmöglichkeiten sollten vom Landesgesetzgeber rechtzeitig genutzt werden, um Rechtssicherheit zur gewährleisten.

Platz für Notizen:

Weitere aktuelle Entwicklungen?

- Derzeit sind im Land NRW leider noch keine aktuellen Entwicklungen bekannt.
- Auf EU-Ebene ist am 10. Januar 2017 der Entwurf für eine EU-ePrivacy-Verordnung veröffentlicht worden.
  - Dieser wird derzeit vom EU-Parlament und vom EU-Rat beraten
  - Hierzu liegt ein erster Entwurf der Berichterstatterin des LIBE-Ausschusses des Parlaments vor
  - Diese Verordnung soll – nach derzeitiger Planung – auch bereits am 25. Mai 2018 gültig werden
  - Sie ersetzt die bisherige ePrivacy-Richtlinie und die entsprechenen nationalen Umsetzungsregelungen

Weitere Informationen zur DSGVO

- Dokumentation des Gesetzgebungsverfahren: http://eur-lex.europa.eu/procedure/DE/201286
- Endfassung des Verordnungsentwurfs in allen Amtsprachen: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=consil%3AST_5419_2016_INIT
- Synopse der DSGVO mit den Artikeln und den zugeordneten Erwägungsgründen sowie den entsprechenden Paragraphen des ab dem 25. Mai 2018 geltenden BDSG: https://efweha-verlag.de/bd41
- Weitere Links finden sich auf http://dvd-ev.de/eudsgvo.htm
- https://dsgvo.expert

Platz für Notizen:

Zum Schluß

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Noch Fragen?

Diplom Informatiker Werner Hülsmann
* Münchener Straße 101 – Geb. 1 /1. OG • D-85737 Ismaning
  Tel.: 089 / 51 30 569-7, FAX: -8
* Kurfürstenstr. 6 • D-12105 Berlin Mariendorf
  Tel.: 030 / 22 43 84 36
Mobil: 0177 / 28 28 681
E-Mail: wh@datenschutzwissen.de
https://datenschutzwissen.de oder https://dsgvo.expert