Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 2. Übung im SoSe 2022:

Einführung in den Datenschutz (2)
& Pandemie

2.1 Privacy by Design & Default

Aufgabe:

- Geben Sie mind. 3 frei gewählte Beispiele, wie nach Art. 25 EU-DSGVO
  a) **Datenschutz durch Technikgestaltung**
  b) **Datenschutz durch datenschutzfreundliche Voreinstellungen** jeweils erreicht werden kann!

2.1 Privacy by Design & Default (1)

a) 3 Beispiele für **Datenschutz durch Technikgestaltung**:

- Die Verarbeitung berücksichtigt eine frühzeitige Pseudonymisierung personenbezogener Daten mit entsprechender Separierung des Zuordnungsmerkmals, ohne dass dies im Verarbeitungssystem selbst wieder zusammengeführt werden kann
- Das Verarbeitungssystem verfügt über Funktionen, die der Betroffene selbst oder über einen Vertreter nutzen kann, um sich die zu seiner Person gespeicherten Daten einsehen zu können
- Die vom Verarbeitungssystem verarbeiteten Daten werden verschlüsselt gespeichert

2.1 Privacy by Design & Default (2)

b) 3 Beispiele für **Datenschutz durch datenschutzfreundliche Voreinstellung**:

- Das Verarbeitungssystem weist Funktionen auf zur Übertragbarkeit (Exportierbarkeit an vom Betroffenen benannten Stellen) von Daten und fristgerechten Löschung der Daten
- Der durch das Verarbeitungssystem verwendete Datenumfang ist auf das absolut Notwendige beschränkt, das zur Zweckerfüllung benötigt wird
- Das Verarbeitungssystem verfügt über ein umfassendes Berechtigungskonzept, mit dem ein differenziertes Berechtigungswesen abgebildet werden kann, das den generellen Zugriff nach dem Need-to-know-Prinzip gewährt und den Zugriff auf besonders schützenswerte Daten nur unter Einhaltung eines 4-Augen-Prinzips zulässt

2.2 Infektionsschutz

Aufgabe:

- Welche Regelungen zur Verarbeitung personenbezogener Daten im Zusammenhang mit Corona (COVID-19 bzw. SARS-CoV-2) sind im **Infektionsschutzgesetz** geregelt?

2.2 Infektionsschutz (1)

- Nach § 2 Nr. 16 IfSG sind personenbezogene Angaben: Name und Vorname, Geschlecht, Geburtsdatum, Anschrift der Hauptwohnung oder des gewöhnlichen Aufenthaltsortes und, falls abweichend, Anschrift des derzeitigen Aufenthaltsortes der betroffenen Person sowie, soweit vorliegend, Telefonnummer und E-Mail-Adresse.
- Nach § 4 Abs. 1 IfSG darf das Robert Koch-Institut zur Erfüllung vorgeschriebener Amtshilfe und nach § 4 Abs. 3 IfSG im Rahmen seiner Aufgaben personenbezogene Daten verarbeiten, soweit es zur Abwendung von Gefahren von Dritten und zum Schutz von unmittelbar Betroffenen im Rahmen der frühzeitigen Erkennung und Verhinderung der Weiterverbreitung von bedrohlichen übertragbaren Krankheiten, der Unterstützung bei der Ausbruchsuntersuchung und -bekämpfung, der Kontaktpersonennachverfolgung oder der medizinischen Evakuierung von Erkrankten und Ansteckungsverdächtigen erforderlich ist.

2.2 Infektionsschutz (2)

- Bei einer gesundheitlichen Notlage von internationaler Tragweite sind nach § 12 Abs. 1 IfSG personenbezogene Angaben unverzüglich dem Robert Koch-Institut zu übermitteln.
- Nach § 13 Abs. 2 IfSG sind personenbezogene Daten, die bereits bei der Vorsorge oder Versorgung erhoben wurden, zu anonymisieren.
- Nach § 14 Abs. 3 IfSG sind personenbezogene Daten, welche ans elektronische Melde- und Informationssystem übertragen wurden, zu pseudonymisieren. Verschlüsselung und Authentifizierung haben dabei nach § 14 Abs. 6 IfSG dem Stand der Technik zu entsprechen.
- Angaben über festgestellte Impfreaktionen sind nach § 11 Abs. 4 IfSG an das Paul-Ehrlich-Institut zu übermitteln und dort zu pseudonymisieren (Geburtsdatum, Geschlecht sowie der erste Buchstabe des ersten Vornamens und der erste Buchstabe des ersten Nachnamens).
- Besteht der Verdacht, dass ein Arzneimittel Quelle einer Infektion ist, sind entsprechende Daten an das Paul-Ehrlich-Institut bzw. Bundesinstitut für Arzneimittel und Medizinprodukte vom Gesundheitsamt nach § 27 Abs. 5 IfSG zu übermitteln und dort analog zu pseudonymiseren.

2.2 Infektionsschutz (3)

- Soweit es zur Verhütung von Infektionen im Sinne von § 2 Nr. 8 IfSG in Bezug auf übertragbare Krankheiten erforderlich ist, darf der Arbeitgeber nach § 23a IfSG personenbezogene Daten eines Beschäftigten über dessen Impf- und Serostatus verarbeiten, um über die Begründung eines Beschäftigungsverhältnisses oder über die Art und Weise einer Beschäftigung zu entscheiden.
- Nach § 28a Abs. 4 IfSG dürfen von den Verantwortlichen im Rahmen der Kontaktdatenerhebung von Kunden, Gästen oder Veranstaltungsteilnehmern nur personenbezogene Angaben sowie Angaben zum Zeitraum und zum Ort des Aufenthaltes erhoben und verarbeitet werden, soweit dies zur Nachverfolgung von Kontaktpersonen zwingend notwendig ist. Die Verantwortlichen haben sicherzustellen, dass eine Kenntnisnahme der erfassten Daten durch Unbefugte ausgeschlossen ist. Die Daten dürfen nicht zu einem anderen Zweck als der Aushändigung auf Anforderung an die nach Landesrecht für die Erhebung der Daten zuständigen Stellen verwendet werden und sind vier Wochen nach Erhebung zu löschen.

2.3 CoronaVO Studienbetrieb

Aufgabe:

- Welche Regelungen zur Verarbeitung personenbezogener Daten sind hinsichtlich etwaiger Nachweispflichten in der **Corona-Verordnung Studienbetrieb** geregelt?

2.3 CoronaVO Studienbetrieb

- § 6 Abs. 2 CoronaVO Studienbetrieb: Der Hochschulnachweis über einen vorhandenen Impf-, Genesenen- oder Teststatus enthält die Angabe, dass ein Impf-, Genesenen- oder Teststatus […] ab einem oder bis zu einem bestimmten Zeitpunkt vorliegt, den Namen sowie die Matrikelnummer oder das Geburtsdatum. Die Hochschule darf jedoch nur Nachweise mit Pseudonymen im Sinne von Art. 4 Nr. 5 EU-DSGVO speichern.
- § 7 Abs. 1 CoronaVO Studienbetrieb: Gleiches gilt für die Nutzung studentischer Lernplätze sowie für den Zutritt zu Archiven und Bibliotheken.
- Ansonsten dient das Abfragen eines entsprechenden Impf-, Genesenen- oder Teststatus nur einer Beschränkung des Zutritts und führt zu keiner Speicherung personenbezogener Daten.

2.4 Datenschutz-Erklärung zur Big-Data-Analyse

Aufgabe:

- Was ist aus datenschutzrechtlicher Sicht zu beachten, wenn im Sinne des IfSG pseudonymisierte Gesundheitsdaten im Rahmen eines Forschungsprojekts einer **Big Data Analyse** unterziehen werden sollen? Erstellen Sie hierzu eine geeignete **Datenschutzerklärung** im Sinne von Art. 14 EU-DSGVO!

2.4 Datenschutz-Erklärung zur Big-Data-Analyse (1)

Vorbemerkungen:

- Big Data = Verarbeitung umfangreicher Datenmengen
- Datensammlungen weisen i.d.R. unstrukturierte Daten auf, die erst mittels Big Data Processing strukturiert werden sollen
- Ziel ist i.d.R. strukturelle Informationen zu gewinnen, die mit recht hoher Wahrscheinlichkeit Zukunftsprognosen zulassen
- Wurden Datensätze ursprünglich zu unterschiedlichen Zwecken erhoben, ist darauf zu achten, dass die neu verfolgten Zwecke noch mit den ursprünglichen vereinbar sind, sonst ist eine Anonymisierung nötig
- Anhand der Datensammlung darf keine automatisierte Einzelentscheidung vorgenommen werden
- Da die Daten für Big Data Analysen i.d.R. nicht beim Betroffenen direkt erhoben werden, sondern aus anderen Datensenken stammen, sind Betroffene nach Art. 14 EU-DSGVO zu informieren

2.4 Datenschutz-Erklärung zur Big-Data-Analyse (2)

Datenschutz-Information nach Art. 14 EU-DSGVO:

Name und Kontaktdaten des Verantwortlichen:

Anschrift: <Anschrift Forschungseinrichtung>
Datenschutzbeauftragter: <Angaben DSB@Forschungseinrichtung>

Zwecke der Verarbeitung und Rechtsgrundlage:

Zweck: Anonymisierte Auswertung pseudonymisierter Gesundheitsdaten zur Ermittlung statistischer Zusammenhänge im Rahmen der Pandemiebekämpfung; keine automatisierte Entscheidung
Rechtsgrundlage: Art. 6 Abs. 1 lit. e EU-DSGVO (öffentliches Interesse; wg. Forschungsprojekt); ergänzend zusätzliches Forschungsprivileg, welches für die Forschungseinrichtung i.V.m. Art. 89 EU-DSGVO zur Anwendung kommt (z.B. § 27 BDSG für Forschungseinrichtung des Bundes bzw. falls nicht-öffentlich, etwa Paul-Ehrlich-Institut i.V.m. § 11 Abs. 4 IfSG sowie § 27 Abs. 5 IfSG, bzw. § 13 LDSG für Forschungseinrichtung des Landes etwa Universität / Universitätsklinikum)

2.4 Datenschutz-Erklärung zur Big-Data-Analyse (3)

Datenschutz-Information nach Art. 14 EU-DSGVO: Fortsetzung

Datenkategorien und Datenherkunft:

pseudonymisierte Gesundheitsdaten nach IfSG durch speichernde Stelle nach IfSG

Empfänger:

interne Stellen zur Aufgabenerledigung
Stelle nach IfSG zur Pandemiebekämpfung
keine Übermittlung in Drittland

Speicherdauer:

Nach Durchführung der Anonymisierung nach § 27 Abs. 3 BDSG bzw. § 13 Abs. 2 LDSG unbegrenzt

Betroffenenrechte:

Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit & Beschwerde bei der Aufsichtsbehörde

2.5 Datenschutzmanagement

Aufgabe:

- Welche Prozesse hat eine Universität zum **Datenschutzmanagement** aufgrund der datenschutzrechtlichen Bestimmungen aus EU-DSGVO unter Berücksichtigung etwaiger Besonderheiten aus IfSG sowie CoronaVO Studienbetrieb umzusetzen?

  Hinweis: Unter Prozesse sind festgelegte, handlungsanleitende Arbeitsschritte zu verstehen, welche sachlich miteinander zusammen hängen. Für das Management wiederum sind nur Steuerungsprozesse maßgeblich. Listen Sie daher nur solche Prozesse auf, die bei der Erfüllung datenschutzrechtlicher Vorschriften eine Steuerungswirkung haben.

2.5 Datenschutzmanagement

- Durchführung vorgeschriebener Datenschutz-Folgenabschätzungen, z.B. zur Pseudonymisierung von Gesundheitsdaten
- Durchführung der Regelkontrolle hinsichtlich der Einhaltung von Datenschutzvorschriften bzw. Pandemie-Vorschriften
- Unterrichtung und Beratung tätiger Personen, z.B. zu Nachweis Impf-, Genesenen- oder Teststatus
- Festlegung geeigneter technischer & organisatorischer Maßnahmen, angemessen zum Schutzbedarf & nach Stand der Technik
- Regelmäßige Überprüfung & Aktualisierung der Maßnahmen
- Erlass geeigneter Datenschutzrichtlinien & universitärer Satzungen, z.B. zur Konsequenz aufgedeckter Verstöße bei durchgeführten Stichproben zur Kontrolle von Nachweisen
- Auswahl geeigneter Auftragsverarbeiter, z.B. für Online-Lehre
- Durchführung vorgeschriebener Meldungen von Datenpannen