Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 2. Übung im SoSe 2021:

Einführung in den Datenschutz
& Pandemie (2)

2.1 Einwilligungserklärung

Aufgabe:

- Formulieren Sie eine **Einwilligungserklärung**, die alle Anforderungen nach Art. 7 EU-DSGVO erfüllt, zur Übermittlung von Schnelltestergebnissen (unter Angabe des Namens, des Datums des durchgeführten Schnelltests und ob dieser Test positiv oder negativ ausfiel) an einen von Ihnen frei gewählten Empfänger zur Vereinbarung eines Vor-Ort-Termins am Folgetag!

2.1 Einwilligungserklärung

Muster einer Einwilligungserklärung:

Hiermit willige ich ein, dass die zu meiner Person gehörenden Angaben zu meinem Namen, dem Datum des innerhalb von 24 Stunden vor dem zu vereinbarenden Termin durchgeführten Schnelltests und des Ergebnisses dieses Schnelltests von der <Bezeichnung des Verantwortlichen> zum Zweck der Vereinbarung eines Vor-Ort-Termins verarbeitet werden dürfen. Ich wurde darüber informiert, dass diese Einwilligung im Rahmen der vorgeschriebenen Speicherbegrenzung zu Nachweiszwecken gespeichert wird und dass ich diese Einwilligung jederzeit mit Wirkung für die Zukunft auf gleiche Weise, wie sie erteilt wurde, widerrufen kann. Mir ist bekannt, dass dies nicht die Rechtmäßigkeit der bisher auf der Grundlage dieser Einwilligung erfolgten Verarbeitung berührt.

2.1 Einwilligungserklärung

Anmerkungen:

- In der CoronaVO sind zahlreiche Stellen aufgeführt, die (bei einer 7-Tage-Inzidenz von unter 100) durch Vorlage eines negativen Schnelltests (und künftig auch einer komplett vorgenommenen Impfung oder eines Nachweises einer ausreichend kurz zurückliegenden Genesung) besucht werden dürfen (z.B. im Rahmen von Click & Meet).
- Ein Schnelltest muss dabei von einem geschulten Dritten durchgeführt oder überwacht werden (z.B. Apotheke) und führt zu einem schnelleren Ergebnis als ein PCR-Test (und ist auch weniger unangenehm in der Durchführung).
- Normalerweise wird ein solcher Nachweis bei Einlass der betreffenden Stelle, die besucht werden soll, vorgelegt, welche sich zuvor von Besuchern versichern lassen, dass diese einen entsprechenden Schnelltest vorlegen oder dort vor Ort zum Eintritt ablegen. Da ein solcher Test Gesundheitsdaten beinhaltet, bedarf eine Vorab-Zusendung einer Einwilligung.

2.2 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!

2.2 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

2.2 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

2.3 Schutzziele

Aufgabe:

- Welche **Schutzziele** müssen Systeme oder Dienste, mit denen personenbezogene Daten verarbeitet werden, berücksichtigen? Ordnen Sie die Angaben aus Art. 32 Abs. 1 lit. c EU-DSGVO und Art. 32 Abs. 2 EU-DSGVO diesen Schutzzielen zu!

2.3 Schutzziele

Schutzziel	Ausprägung
Vertraulichkeit	Keine unbefugte **Offenlegung** von personenbezogenen Daten
	Kein unbefugter **Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet werden
Integrität	Keine unbeabsichtigte oder unrechtmäßige **Veränderung** von personenbezogenen Daten
	Keine unbeabsichtigte oder unrechtmäßige **Vernichtung** von personenbezogenen Daten
	Kein unbeabsichtigter oder unrechtmäßiger **Verlust** von personenbezogenen Daten
Verfügbarkeit	Keine unbeabsichtigte oder unrechtmäßige **Vernichtung** von personenbezogenen Daten
	Kein unbeabsichtigter oder unrechtmäßiger **Verlust** von personenbezogenen Daten
	Rasche **Wiederherstellung** der Verfügbarkeit von bzw. dem Zugang auf personenbezogene Daten bei einem physischen oder technischen Zwischenfall
Belastbarkeit	Rasche **Wiederherstellung** der Verfügbarkeit von bzw. dem Zugang auf personenbezogene Daten bei einem physischen oder technischen Zwischenfall

2.4 Datenschutzverletzung

Aufgabe:

- Was ist im Falle einer **Verletzung des Schutzes von personenbezogenen Daten** zu tun? Begründen Sie Ihre Antwort! (d.h. belegen Sie Ihre Antwort unter Angabe entsprechender Rechtsquellen)

2.4 Datenschutzverletzung (1)

- Unter einer Verletzung des Schutzes personenbezogener Daten ist nach Art. 4 Nr. 12 EU-DSGVO zu verstehen eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig
  - zur **Vernichtung** von personenbezogenen Daten,
  - zum **Verlust** von personenbezogenen Daten,
  - zur **Veränderung** von personenbezogenen Daten,
  - zur **unbefugten Offenlegung** von personenbezogenen Daten oder
  - zum **unbefugten Zugang** zu personenbezogenen Daten

  führt, die übermittelt, gespeichert oder sonstige Weise verarbeitet wurden
  → Sicherheit der Verarbeitung nach Art. 32 EU-DSGVO verletzt
  → betrifft sowohl eine absichtliche Verletzung (→ Angriff von Intern oder Extern) als auch eine versehentliche Verletzung (→ Fahrlässigkeit)
- Solche Fälle sind binnen 72 Stunden der Aufsichtsbehörde nach Art. 33 EU-DSGVO zu melden und darüber u.U. unverzüglich die betroffene Person nach Art. 34 EU-DSGVO zu benachrichtigen

2.4 Datenschutzverletzung (2)

- Die Meldung nach Art. 33 Abs. 1 EU-DSGVO muss erfolgen, es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen
  → Verantwortlicher muss Verletzung erst mal feststellen
  → Verantwortlicher muss entsprechende Detektions- und Meldeprozesse etablieren
  → Nach Feststellung ist zunächst zu prüfen, ob aus der Verletzung ein Risiko für die Rechte und Freiheiten mind. 1 natürlicher Person resultieren kann
  → Nach ErwG 85 EU-DSGVO geht nur dann kein Risiko von einer Datenschutzverletzung aus, wenn der Verantwortliche dies selbst nach Art. 5 Abs. 2 EU-DSGVO nachweisen kann
- Auftragsverarbeiter haben den Verantwortlichen eine Datenschutzverletzung unverzüglich zu melden nach Art. 33 Abs. 2 EU-DSGVO
- Meldungen an die Aufsichtsbehörde haben nach Art. 33 Abs. 3 EU-DSGVO folgende Informationen zu enthalten:
  - Beschreibung der Art der Datenschutzverletzung, möglichst mit Angabe der Kategorie und ungefähren Zahl betroffener Personen als auch mit Angabe der Kategorie und ungefähren Zahl betroffener Datensätze

2.4 Datenschutzverletzung (3)

- Meldungen an die Aufsichtsbehörde haben nach Art. 33 Abs. 3 EU-DSGVO folgende Informationen zu enthalten: (Fortsetzung)
  - Namen und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
  - Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung
  - Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und ggf. von Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkung

  → Datenschutzverletzung ist näher zu analysieren (Betroffene & Datenarten)
  → Analyse der wahrscheinlichen Folgen
  → Gewichtung potenzieller Folgen hinsichtlich Eintrittswahrscheinlichkeit
  → Prüfung, welche Maßnahmen zur Behebung der Datenschutzverletzung zu ergreifen sind
  → Verhinderung einer Wiederholungsgefahr
  → Abmilderung negativer Folgen für Betroffene
- Datenschutzverletzungen sind zu dokumentieren nach Art. 33 Abs. 5 EU-DSGVO

2.4 Datenschutzverletzung (4)

- Wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, hat der Verantwortliche nach Art. 34 Abs. 1 EU-DSGVO die betroffene Person unverzüglich und nach Art. 34 Abs. 2 EU-DSGVO in klarer und einfacher Sprache mit den gleichen Informationen zu benachrichtigen
  → Bewertung des Risikos für die persönlichen Rechte und Freiheiten der Betroffenen zu ermitteln
  → Berücksichtigung der individuellen Risiken (→ keine globale Betrachtung)
- Eine Benachrichtigung der betroffenen Personen ist nicht erforderlich, wenn
  - der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen vor der Datenschutzverletzung getroffen hat, die einen unbefugten Zugang zu den Daten verhindern sollen (→ präventiver Schutz)
  - der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht (→ reaktiver Schutz)
  - die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre (→ dann: öffentliche Bekanntmachung nötig)

2.5 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!

2.5 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

2.5 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)

2.5 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