Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 3. Übung im SoSe 2021:

Einführung in den Datenschutz
& Pandemie (3)

3.1 Datenschutzerklärung

Aufgabe:

- Die Lehrveranstaltung einer Universität soll infolge der Pandemie auf reine Online-Lehre umgestellt werden. Hierzu soll sowohl zur Vorlesung als auch zur Übung ZOOM mit einer Zugangsbeschränkung eingesetzt werden. Entwerfen Sie eine zugehörige **Datenschutzerklärung** zum Einsatz von ZOOM im Sinne von Art. 13 EU-DSGVO!

3.1 Datenschutzerklärung (1)

- Zur Online-Lehre an der Universität werden Vorlesungen und Übungen mittels Online-Tool ZOOM abgewickelt, welches von der Zoom Video Communications, Inc. auf der Grundlage einer Datenschutzvereinbarung unter Einsatz eines Data Centers auf dem Gebiet der EU samt zugehöriger Standard-Datenschutz-Klauseln für etwaige Datenexporte außerhalb der EU und des EWR betrieben wird. Details zur Datenverarbeitung durch ZOOM kann der zugehörigen Datenschutzrichtlinie auf **https://zoom.us/privacy** entnommen werden. Dabei besteht hinsichtlich der Meeting-Metadaten ein Datentransfer in die USA.
- Dieses Online-Tools ist bereits durch Aufruf eines zugesandten Links im Browser nutzbar. Alternativ kann lokal auch eine entsprechende App installiert werden. In beiden Fällen ist ein Aufruf der Webseite des Anbieters bzw. der Universität unter Ausnutzung der universitären Lizenz zumindest initial erforderlich.
- Die Online-Lehre wird unter Ausnutzung einer Zugangsbeschränkung durchgeführt, weshalb die entsprechenden Links stets der Eingabe der lehrveranstaltungsspezifischen Meeting-ID und des zugehörigen Kenncodes bedarf, die vom Organisator der betreffenden Lehrveranstaltung zur Verfügung gestellt wird.

3.1 Datenschutzerklärung (2)

- Bei Nutzung von ZOOM werden gespeichert:
  - Angaben zum Benutzer, bestehend aus IP-Adresse, Verbindungsbeginn und -ende, bei Beginn der Veranstaltung selbst eingegebene Nutzerkennung
  - Meeting-Metadaten: Thema, Beschreibung (optional), Teilnehmer IP-Adressen, Geräte-/ Hardware-Informationen
  - Bei Einwahl mit dem Telefon: Angabe zur eingehenden und ausgehenden Rufnummer, Ländername, Start- und Endzeit
  - Bei Eingabe von Chatnachrichten, dem Upload von Dateien oder dem Teilen von Bildschirminhalten: Entsprechende Angaben, die vom Benutzer selbst hierzu ausdrücklich preisgegeben werden
  - Bei Aktivieren des Mikrofons: Tondaten, die vom genutzten Mikrofon seitens des Benutzers aufgezeichnet werden
  - Bei Aktivieren der Kamera: Bilddaten, die von der genutzten Kamera seitens des Benutzers aufgezeichnet werden
- Die mittels ZOOM abgewickelte Online-Lehre wird defaultmäßig nicht und ansonsten nur mit Zustimmung aller Beteiligten aufgezeichnet.

3.1 Datenschutzerklärung (3)

- Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen der Nutzung von ZOOM zur universitären Online-Lehre ist Art. 6 Abs. 1 lit. e EU-DSGVO.
- Nach Abschluss der jeweiligen Lehrveranstaltungssessions werden die jeweils gespeicherten Daten automatisch gelöscht. Alle weiteren Speicherdauern richten sich ansonsten nach den Vorgaben für Telemediendienste zu audiovisuellen Nutzungsdaten.
- Die Teilnehmenden einer Lehrveranstaltung, die mittels ZOOM abgewickelt wird, sind dazu aufgerufen, im Rahmen der jeweiligen Sessions nur erforderliche Daten preiszugeben. Das betrifft ausdrücklich auch den gewählten Bildausschnitt (evtl. unter Ausnutzung von Blurring), vorgeführte Bildschirminhalte und die übertragenen Hintergrundgeräusche während das eigene Mikrofon aktiviert ist.
- Alle weiteren Details zu den Betroffenenrechten und den Angaben zum Verantwortlichen kann der **allgemeinen Datenschutzerklärung der Universität** entnommen werden.

3.2 Löschkonzept

Aufgabe:

- Entwerfen Sie unter Beachtung telemedienrechtlicher Vorschriften ein **Löschungskonzept** für eine Mailingliste, zu der sich Abonnenten frei eintragen können und die über ein Archiv zugesandter Mails verfügt, welches für alle Abonnenten nach Eingabe frei gewählter Zugangsdaten zugänglich ist! Berücksichtigen Sie dabei auch, wie mit Datensicherungen umzugehen ist.

3.2 Löschkonzept (1)

- Eine Mailingliste ist ein Telemediendienst
  → Neben den allgemeinen Datenschutzvorschriften aus der EU-DSGVO treten insoweit telemedienrechtliche Vorschriften aus dem TMG hinzu
  (aktueller Hinweis: Derzeit werden vom Gesetzgeber diese Vorschriften geändert und in einem TTDSG gebündelt; auf EU-Ebene steht wiederum eine Verabschiedung der ePrivacy-Verordnung vor dem Abschluss)
- Die Speicherbegrenzung aus Art. 5 Abs. 1 lit. e EU-DSGVO bezieht sich auf Identifizierungsdaten
- Nach Art. 17 Abs. 1 lit. a EU-DSGVO sind personenbezogene Daten zu löschen, wenn sie für die festgelegten Zwecke nicht mehr notwendig sind
- Nach Art. 30 Abs. 1 lit. f EU-DSGVO sind im Verzeichnis von Verarbeitungstätigkeiten die Regellöschungsfristen festzuhalten

3.2 Löschkonzept (2)

- Für Löschungskonzept ist vor allem der Umgang mit dem Mailinglisten-Archiv zu regeln, welches durch die jeweils aktuellen Abonnenten unter Eingabe frei gewählter Zugangsdaten einsehbar ist.
- Das Mailinglisten-Archiv besteht jedoch unabhängig von dem individuellen Abonnement des einzelnen Mitglieds der Mailingliste!
  → Zugehörige Datenschutzerklärung muss ausdrücklich definieren, wie mit entsprechenden Beiträgen ausgeschiedener Abonnenten umgegangen wird; hierbei kann unterschieden werden zwischen den aufrufbaren Header-Daten (welche z.B. mittels Pseudonymisierung vom unmittelbaren Personenbezug befreit werden können) und den Inhalts-Daten, die jedoch nur schwer von spezifischen Angaben befreit werden können, zumal sich weitere Antworten ja mit Zitierung entsprechender Bestandteile kaum noch entsprechend zuordnen lassen!

3.2 Löschkonzept (3)

- In der Einwilligungserklärung zum Abonnement der Mailingliste muss daher die Speicherung gesendeter Beiträge und deren Ablage im Mailinglisten-Archiv von der abonnementsbezogenen Löschung ausdrücklich ausgenommen werden!
- Zum Ausgleich muss aber die Möglichkeit für Abonnenten bestehen, Beiträge, in denen diese ohne ihre Zustimmung bzw. ohne Referenz auf selbst eingestellte Beiträge genannt werden, auf Anforderung löschen zu lassen → Teil des Löschkonzepts
- Die EU-DSGVO bestimmt jedoch nicht exakt, was unter „Löschen“ zu verstehen ist
- Nach ErwG 39 muss sichergestellt sein, dass Unbefugte keinen Zugang zu den Daten haben und diese Daten auch nicht nutzen können
  → reiner Leserechteentzug nicht ausreichend
  → Pseudonymisierung dagegen u.U. schon

3.2 Löschkonzept (4)

- Im Rahmen der Datenschutzerklärung ist folglich festzulegen, ab wann ein Thread, der aus den zu dem betreffenden Thema über die Mailingliste gesandten Beiträgen besteht, aus dem Mailinglisten-Archiv automatisiert gelöscht wird, z.B. max. nach 6 Jahren (analog zur Aufbewahrungspflicht für Geschäftsbriefe) nach letztem Beitrag in einem betreffenden Thread (i.d.R. wird für ein Mailinglisten-Archiv auch eine kürzere Frist, z.B. 3 Jahre analog zu üblichen Zertifizierungsfristen, ausreichend sein)
  → im Löschkonzept ist entsprechend auszuführen, wie die automatisierte Löschung dann erfolgt
- Mailinglisten-Archivierung setzt jedoch Datensicherung voraus
- Datensicherung = Maßnahme im Sinne von Art. 32 Abs. 1 lit. b und c EU-DSGVO i.V.m. Art. 6 Abs. 1 lit. f EU-DSGVO

3.2 Löschkonzept (5)

- Für Datensicherungen gelten die Fristen des Hauptverfahrens analog, doch müssen Daten nicht gesondert von Datensicherungsmedien entfernt werden (aus technischen Gründen auch schwerlich möglich); hier bestimmt sich die Aufbewahrungsfrist nach der längstbenötigten Frist des Mediums, wobei diese allerdings nicht künstlich erhöht werden darf, indem unnötig Daten hinzugespeichert werden, die eine deutlich längere Aufbewahrungsfrist benötigen (würde sonst dem Grundsatz von Treu und Glauben nach Art. 5 Abs. 1 lit. a EU-DSGVO und andererseits der Datenminimierung nach Art. 5 Abs. 1 lit. c EU-DSGVO widersprechen)

3.2 Löschkonzept (6)

- Nach § 35 Abs. 1 BDSG 2018 ist (auf Basis von Art. 23 Abs. 1 lit. j EU-DSGVO) für eine Datensicherung die Einschränkung (= Sperrung) der Datensicherungsdaten ausreichend, da hierfür (im Gegensatz zu den Archivdaten) das Interesse des Betroffenen an der Löschung von vorneherein als gering anzusehen ist und eine Löschung wegen der besonderen Art der Speicherung nur mit unverhältnismäßig hohem Aufwand möglich wäre (sequentielles Umkopieren auf ein anderes Datensicherungsmedium mit dem zusätzlichen Risiko, dass durch Umkopieren ggf. die weiter aufzubewahrenden Daten nicht mehr lesbar sind)

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung I

Aufgabe:

- Für ein **Pandemie-Web-Portal** wurde Folgendes geplant:
  - Das Web-Portal soll auf Gesundheitsdaten aus der Pandemie-Datenbank lesend zugreifen können, wobei nur die Betroffenen unmittelbar ihre eigenen personenbezogenen Daten und alle anderen Stellen nur pseudonymisierte Gesundheitsdaten sowie weitere Daten sehen, die jeweils hinzugespeichert worden sind
  - Die Betroffenen, welche in der Pandemie-Datenbank erfasst sind, sollen eine fortlaufende Nummer als Benutzerkennung erhalten und das Web-Portal nach Eingabe eines frei gewählten Passwortes nutzen können, um ergänzende Angaben zu relevanten Begleitumstände selbst eingeben zu können
  - Betroffene sollen ihre Eingaben nach Eintragung per Mail erhalten
  - Im Web-Portal sollen die Betroffenen sehen können, wie Rahmenbedingungen (begünstigende und beeinträchtigende Faktoren), Impfentwicklungen und Krankheitsverläufe bei anhand vordefinierter Kriterien als vergleichbar geltenden Patienten ausgesehen haben
  - Das Web-Portal soll als Public Cloud implementiert werden

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung II

Aufgabe: (Fortsetzung)

- Geben Sie an, welche potenziellen Datenschutzrisiken Sie im Rahmen einer Datenschutz-Folgenabschätzung (gem. Art. 35 EU-DSGVO) sehen (unter Berücksichtigung der Bußgeldbestimmungen und Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten), schätzen Sie die Eintrittsstufe dieser Datenschutzrisiken ab und ermitteln Sie den Handlungsbedarf gemäß nächstehender 3x3-Risk-Map. Sofern Handlungsbedarf besteht, geben Sie eine passende, zu ergreifende Schutzmaßnahme an.

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (1)

1) Ermittlung potenzieller Datenschutzrisiken:

- Lesender Zugriff auf eigene Daten im Web-Portal auf Pandemiedaten
  1. Pandemiedaten offensichtlich auf Betroffene zuordnenbar → Gefahr: Unbefugte Offenlegung ggf. möglich (Art. 32 Abs. 2 EU-DSGVO → Bußgeld nach Art. 83 Abs. 4 lit. a EU-DSGVO)
- Benutzerkennung via fortlaufender Nummer & freie Passwortwahl
  2. Enumerative Zugangsdaten → Gefahr: kein unmittelbarer Schaden
  3. Mangelnder Zugriffsschutz bei geringer Passwortgüte → Gefahr: Unbefugter Zugang (Art. 32 Abs. 2 EU-DSGVO → Bußgeld nach Art. 83 Abs. 4 lit. a EU-DSGVO)
- Bestätigungsmail für durchgeführte Eingaben
  4. Mail-Server mit Web-Portal direkt verbunden → Gefahr: kein unmittelbarer Schaden
- Einsicht in Vergleichsdaten via Web-Portal
  5. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil → Gefahr: Profiling (formaler Verstoß, da durch diese DSFA ja behandelt)

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (2)

1) Ermittlung potenzieller Datenschutzrisiken: (Fortsetzung)

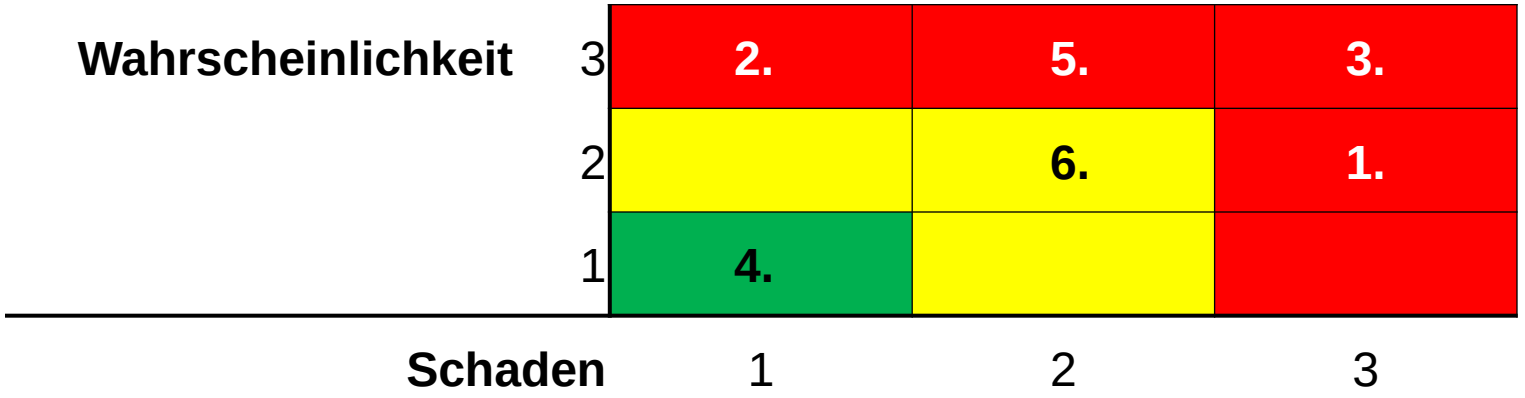
- Web-Portal als Public Cloud implementiert
  6. Pandemiedaten unzureichend geschützt → Gefahr: Unbefugte Offenlegung ggf. möglich (Art. 32 Abs. 2 EU-DSGVO → Bußgeld nach Art. 83 Abs. 4 lit. a EU-DSGVO)

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (3)

2) Abschätzung der Eintrittsstufe:

1. Zuordnenbare Pandemiedaten: Gefahreintritt wahrscheinlich, da Angreifer nur über begrenzte Fähigkeiten & Ressourcen verfügen muss, um Daten z.B. via SQL-Injection abrufen zu können, da Daten ja durch den Nutzer eigegeben werden können
2. Enumerative Zugangsdaten: Gefahreintritt sicher, da entsprechendes Ausprobieren voraussetzungslos möglich ist
3. Mangelnder Zugriffsschutz bei geringer Passwortgüte: Gefahreintritt sicher, da Passwort-Cracker leicht downloadbar sind & schlechte Passwörter i.d.R. bereits leicht zum Erfolg führen (z.B. Benutzerkennung = Passwort)
4. Mail-Server mit Web-Portal direkt verbunden: Gefahreintritt nur möglich, da Angreifer erst noch den Verbindungspfad ermitteln muss
5. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil: Gefahreintritt sicher, aufgrund der Voraussetzungen aus 2. & 3.
6. Implementation via Public Cloud: Gefahreintritt wahrscheinlich, da i.d.R. preisgünstig aufgrund geringerer Schutzvorkehrungen

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (4)



Rot = Aktivität nötig; **Gelb** = Aktivität prüfen; **Grün** = Akzeptabel

Wahrscheinlichkeit: **Eintritt einer Verletzung des Schutzes personenbezogener Daten**	**Schaden:** **Grad der Verletzung des Schutzes personenbezogener Daten**
1 = möglich	1 = niedrig (ohne unmittelbare Wirkung)
2 = wahrscheinlich	2 = mittel (formaler Verstoß)
3 = sicher	3 = hoch (Bußgeld/Meldepflicht)

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (5)

3) Handlungsempfehlung:

1. Unbeschränkter Zugriff auf alle personenbezogene Pandemie-Daten
   → Datenvalidierung sicherstellen (SQL-Injection verhindert) & Zuordnungsdaten mittels Broker schützen
2. Enumerative Zugangsdaten
   → Benutzerkennung frei wählen lassen
3. Mangelnder Zugriffsschutz bei geringer Passwortgüte
   → Mindestvorgaben für Passwortgüte festlegen (Komplexität, Länge)
4. Mail-Server mit Web-Portal direkt verbunden
   → akzeptierbar, wenn Verbindungspfad nicht ermittelbar ist und ein Angreifer nicht als Man-in-the-Middle zwischenschalten kann
5. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil
   → nach Änderung zu 2. & 3. ggf. akzeptierbar

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (6)

3) Handlungsempfehlung: (Fortsetzung)

6. Web-Portal mit Pandemiedaten als Public Cloud
   → Einsatz einer Private Cloud, um Schutzvorkehrungen angemessen für Gesundheitsdaten treffen zu können (oder Auswahl einer Public Cloud, die entsprechende Garantien zusichert)

Anmerkung:

- *Die Angabe der Punkte aus Art. 35 Abs. 7 EU-DSGVO ist bei der Durchführung von Datenschutz-Folgenabschätzungen verpflichtend*
  ° auf systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen
  in der Aufgabe jedoch verzichtet, da nach Aufgabenstellung nicht zwingend verlangt

3.4 Vorkehrungen gegen hohe Risiken

Aufgabe:

- Geben Sie fünf frei wählbare Beispiele hinsichtlich des Umgangs mit pseudonymisierten Gesundheitsdaten an, bei denen grundsätzlich ein **hohes Risiko** für die Rechte und Freiheiten der Betroffenen bestehen kann und skizzieren Sie zu treffende **Vorkehrungen**, die bei diesen Beispielen durch den Verantwortlichen getroffen werden müssen, um entweder die Höhe eines potenziellen Schadens oder die Eintrittswahrscheinlichkeit eines solchen Schadens entweder vermeiden oder zumindest ausreichend mindern zu können. Begründen Sie Ihre Antwort und geben Sie insbesondere an, wie die von Ihnen vorgeschlagene Vorkehrung hinsichtlich des Risikos wirkt!

3.4 Vorkehrungen gegen hohe Risiken (1)

1. Beispiel: Die Betroffenen, über die pseudonymisierte Gesundheitsdaten vorliegen, ist unter Berücksichtigung der Namenskürzel, des Geschlechts und der Geburtsdaten im Falle eigener Beschäftigter bei geringer Anzahl reperso-nalisierbar

- **Abschätzung Schaden: hoch!** Unzulässiger Umgang mit Gesundheitsdaten nach Art. 83 Abs. 5 lit. a EU-DSGVO sogar mit hohem Bußgeld bestrafbar
- **Abschätzung Eintrittswahrscheinlichkeit: hoch!** Personenidentifizierende Daten liegen dem Verantwortlichen über seine Beschäftigten unmittelbar vor; bei geringer Anzahl Beschäftigter ist die Eintrittswahrscheinlichkeit faktisch sicher, dass die IfSG-Pseudonyme repersonalisiert werden können
- **Vorkehrung**: Keine Speicherung über Pandemiedaten zu den Beschäftigten
- **Wirkung: Minderung Schaden auf niedrig und Eintrittswahrscheinlichkeit auf niedrig!** Daten, die erst gar nicht erhoben werden, können nicht rechtswid-rig verwendet werden.

3.4 Vorkehrungen gegen hohe Risiken (2)

2. Beispiel: Für neuen Zweck Verknüpfung von Profildaten aus unterschiedlichen Datensammlungen zu nicht miteinander vereinbaren Zwecken

- **Abschätzung Schaden: hoch!** Verstoß gegen Grundsatz aus Art. 5 Abs. 1 lit. b EU-DSGVO, bußgeldbewährt nach Art. 83 Abs. 5 lit. a EU-DSGVO
- **Abschätzung Eintrittswahrscheinlichkeit: hoch!** Unterschiedslose Verknüpfung aller vorhanden Daten führt sicher zur Datenschutzverletzung, da folglich dann keine angemessenen Schutzvorkehrungen getroffen wurden
- **Vorkehrung**: Wo die Zwecke miteinander vereinbar sind, angemessenen rollenbasierten Zugriffsschutz implementieren, um Missbrauchspotenzial zu reduzieren, ansonsten keine unvereinbaren Zwecke miteinander kombinieren
- **Wirkung: Minderung Schaden auf mittel und Eintrittswahrscheinlichkeit auf mittel!** Wenn Zwecke soweit miteinander vereinbar sind, entfällt das Bußgeldrisiko; durch Zugriffsschutz und Beschränkung auf zulässige Verknüpfungen neben Pseudonymisierung sind soweit angemessene Maßnahme getroffen

3.4 Vorkehrungen gegen hohe Risiken (3)

3. Beispiel: Erstellung eines umfassenden Profils unter Einbeziehung von Daten zur Repersonalisierung

- **Abschätzung Schaden: hoch!** Gesundheitsdaten besonders schützenswert und nur unter den Voraussetzungen aus Art. 9 Abs. 2 EU-DSGVO verwendbar; aufgrund der Pseudonymisierung nach IfSG nicht zwingend sichergestellt, dass nur Beschäfigte mit entsprechendem Berufsgeheimnis auf diese Daten zugreifen können
- **Abschätzung Eintrittswahrscheinlichkeit: mittel!** Qualitativ hochwertige Profildaten für Unbefugten u.U. ausreichend interessant, muss aber erst mal Zugriff auf Daten erhalten
- **Vorkehrung**: Keine Zuspeicherung von Repersonalisierungsdaten zulassen und pseudonymisierte Gesundheitsdaten auch nur durch Beschäftigte mit entsprechendem Berufsgeheimnis verarbeiten lassen
- **Wirkung: Minderung Schaden auf mittel!** Angreifer muss selbst über Daten zur Repersonalisierung verfügen, um angereicherte Profildaten missbrauchen zu können

3.4 Vorkehrungen gegen hohe Risiken (4)

4. Beispiel: Studien zur Wirkung von Impfungen leicht repersonalisierbar und aufgrund Zusatzdaten über Vorerkrankungen als Profiling anzusehen

- **Abschätzung Schaden: hoch!** Gesundheitsdaten besonders schützenswert; für Impfstudien werden zudem bestehende Vorerkrankungen hinzugespeichert; durch Angaben der Pseudonymisierung nach IfSG und den recht geringen Fall-zahlen der Vergleichsstudien (Placebo und Impfung) Repersonalisierung leicht möglich
- **Abschätzung Eintrittswahrscheinlichkeit: mittel!** Datensätze i.d.R. nur für Personal mit entsprechendem Berufsgeheimnis zugreifbar; Gesundheitswesen jedoch meist nicht allzu gut abgesichert
- **Vorkehrung**: Erhöhter Zugriffsschutz durch Zwei-Faktor-Authentifizierung von Zugriffsbefugten
- **Wirkung: Minderung Eintrittswahrscheinlichkeit auf niedrig!** Angreifer muss sich beide Faktoren aneignen, um angereicherte Profildaten missbrauchen zu können

3.4 Vorkehrungen gegen hohe Risiken (5)

5. Beispiel: Unzureichende Regelungen zum Umgang mit pseudonymisierten Gesundheitsdaten

- **Abschätzung Schaden: mittel!** Wenn den Personen, die mit besonders schützenswerten Daten umgehen sollen, wichtige Regeln unbekannt sind, worauf sie zu achten haben, werden derartige Fälle früher oder später auftreten
- **Abschätzung Eintrittswahrscheinlichkeit: hoch!** Fehlende Vorgaben führen sicher zumindest zu fahrlässigem Handeln, da unbekannt ist, wie vorzugehen ist
- **Vorkehrung**: Festlegung verbindlicher Vorgaben zum Umgang mit pseudonymisierten Gesundheitsdaten und deren Schulung an den verarbeitenden Personen
- **Wirkung: Minderung Eintrittswahrscheinlichkeit auf mittel!** Versehentliche Fehler beim Umgang mit Daten sind nie ganz ausschließbar, aber spürbar reduziert, wenn ausreichend sprechend formuliert und geschult

3.5 Datenschutzmanagement

Aufgabe:

- Welche Prozesse hat ein Unternehmen zum **Datenschutzmanagement** aufgrund der datenschutzrechtlichen Bestimmungen aus EU-DSGVO unter Berücksichtigung etwaiger Besonderheiten aus IfSG & CoronaVO (einerseits in Bezug auf eigene Beschäftigte und andererseits in Bezug auf Kontakte mit Dritten) umzusetzen?
  Hinweis: Orientieren Sie sich dabei an den Aufgaben, die der Datenschutzbeauftragte in Zusammenarbeit mit anderen Stellen im Unternehmen beim Datenschutz zu erfüllen hat.

3.5 Datenschutzmanagement (1)

Prozesse zum Management des Datenschutzes nach EU-DSGVO:

- **Führung des Verzeichnisses von Verarbeitungstätigkeiten** nach Art. 30 Abs. 1 EU-DSGVO durch Verantwortliche bzw. nach Art. 30 Abs. 2 EU-DSGVO durch Auftragsverarbeiter
- **Benennung eines Datenschutzbeauftragten** nach Art. 37 Abs. 1 EU-DSGVO
- **Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten** nach Art. 37 Abs. 7 EU-DSGVO
- **Datenschutz-Folgenabschätzung** von Verarbeitungen, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen aufweisen können nach Art. 35 Abs. 1 EU-DSGVO, wovon im Zusammenhang mit Pandemiedaten auszugehen ist, unter Beteiligung des Datenschutzbeauftragten nach Art. 35 Abs. 2 EU-DSGVO
  → neue Verfahren beim Datenschutzbeauftragten anmelden!
  → Angaben aus Verzeichnis von Verarbeitungstätigkeiten melden (inkl. geplanter Maßnahmen zur Sicherheit der Verarbeitung nach Art. 32 EU-DSGVO)
  → Angaben über verfolgte berechtigte Interessen, Datenfluss und Zugriffsrollen
  → Rat des Datenschutzbeauftragten einholen! (Art. 39 Abs. 1 lit. c EU-DSGVO)
  → Bewertung Notwendigkeit, Verhältnismäßigkeit & Risiken

3.5 Datenschutzmanagement (2)

Prozesse zum Management des Datenschutzes n. EU-DSGVO: 1. Forts.

- **Regelkontrolle zur Überwachung** der Einhaltung datenschutzrechtlicher Vorschriften nach Art. 39 Abs. 1 lit. b EU-DSGVO
  → Datenschutzbeauftragten rechtzeitig über bestehende & geplante Verarbeitung unterrichten nach Art. 38 Abs. 1 EU-DSGVO!
  → i.d.R. durch Verzeichnis von Verarbeitungstätigkeiten
  → unter Berücksichtigung der Risiken nach Art. 39 Abs. 2 EU-DSGVO
- **Unterrichtung und Beratung der** bei der Verarbeitung personenbezogener Daten **tätigen Personen über ihre datenschutzrechtlichen Pflichten** nach Art. 39 Abs. 1 lit. a EU-DSGVO:
  → Schulungen & Sensibilisierungen nach Art. 39 Abs. 1 lit. b EU-DSGVO
  → Informationsschriften / Merkblätter
  → Belehrungen
  → unter Berücksichtigung der Risiken nach Art. 39 Abs. 2 EU-DSGVO
- **Unterstützung des Datenschutzbeauftragten** durch erforderliches Hilfspersonal sowie Räume, Einrichtungen, Geräte, Mittel und Fortbildungen nach Art. 38 Abs. 2 EU-DSGVO
- **Bearbeitung von Betroffenenanliegen** nach Art. 38 Abs. 4 EU-DSGVO

3.5 Datenschutzmanagement (3)

Prozesse zum Management des Datenschutzes n. EU-DSGVO: 2. Forts.

- **Festlegung geeigneter technischen und organisatorischer Maßnahmen** nach Art. 32 EU-DSGVO unter Berücksichtigung der Risiken nach Art. 24 Abs. 1 EU-DSGVO (Pandemiedaten erfordern höheren Schutzbedarf; Verarbeitung von Impf-stati von Beschäftigten im Sinne von § 23a IfSG möglichst vermeiden)
- **Nachweisführung zur Einhaltung der EU-DSGVO** nach Art. 24 Abs. 1 EU-DSGVO
- **Regelmäßige Überprüfung und Aktualisierung der Schutzvorkehrungen** nach Art. 24 Abs. 1 EU-DSGVO
- **Erlass geeigneter Datenschutzrichtlinien** nach Art. 24 Abs. 2 EU-DSGVO, z.B. zu Prozedere der Verarbeitung von Gesundheitsdaten nach § 8 Abs. 2 CoronaVO
- **Auswahl geeigneter Auftragnehmer, deren Beratung und Überprüfung** nach Art. 28 Abs. 1 und Art. 39 Abs. 1 lit. a & b EU-DSGVO
- **Unterstützung bei den Abwägungen** nach Art. 6 Abs. 1 lit. f EU-DSGVO
- **Unterstützung bei der Meldung von Datenpannen** nach Art. 33 EU-DSGVO
- **Zusammenarbeit mit der Aufsichtsbehörde** nach Art. 39 Abs. 1 lit. d EU-DSGVO
- **Unterstützung bei der Bestimmung erforderlicher Sorgfalt** zur Vermeidung von Schadensersatz nach Art. 82 Abs. 3 EU-DSGVO