Grundlagen des Datenschutzes und der IT-Sicherheit

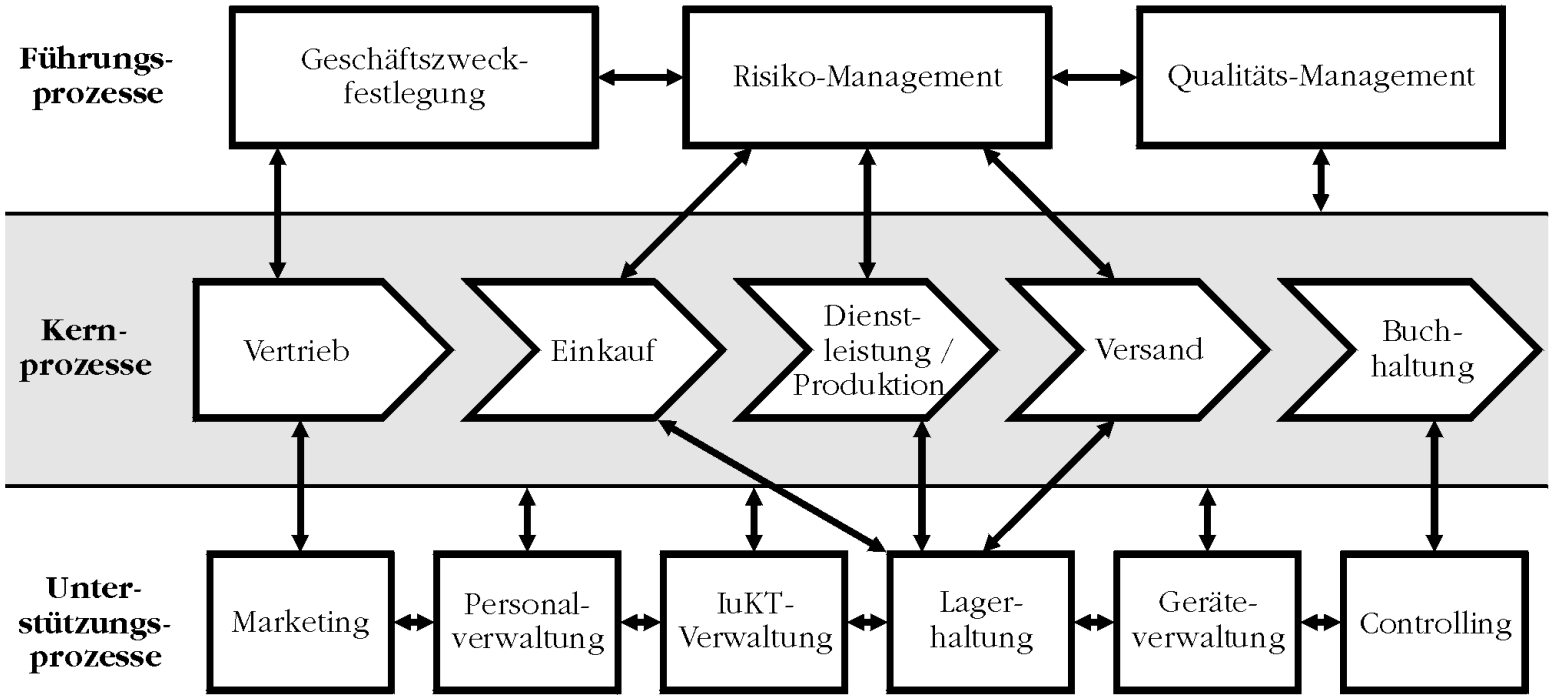
Musterlösung zur 2. Übung im SoSe 2023:

Einführung in den Datenschutz (2)
& OTT-Dienste

2.1 Verfahren I

Aufgabe:

- Für ein Unternehmen wurde folgende Prozesslandkarte ermittelt:



2.1 Verfahren II

Aufgabe:

- Zählen Sie je fünf grundlegende **Verfahren zur Verarbeitung personenbezogener Daten** auf, die von diesem Unternehmen damit im Einsatz sind zur
  a) Verarbeitung personenbezogener Beschäftigtendaten
  b) Verarbeitung personenbezogener Kundendaten

2.1 Verfahren

Beschäftigtendaten-verarbeitung

Personalverwaltung:

- Bewerbungsverfahren
- Personalaktenführung
- Arbeitszeitüberwachung

Buchhaltung:

- Lohn- und Gehaltsabrechnung

Dienstleistung / Produktion:

- Betriebsdatenerfassung

Qualitäts-Management:

- Qualitätskontrolle

Controlling:

- Leistungskontrolle

IuKT-Verwaltung:

- Elektronische Kommunikation

Kundendaten-verarbeitung

Marketing:

- Kundengewinnung (Messen & Gewinnspiele)
- Kundenbewerbung & Newsletter
- Kundendatenanalyse (Tracking)

Vertrieb:

- Vertragsabwicklung
- Customer Relationship Management

Buchhaltung:

- Zahlungsüberwachung

Versand:

- Versand

IuKT-Verwaltung:

- Elektronische Kommunikation

2.2 Datenschutzmanagement I

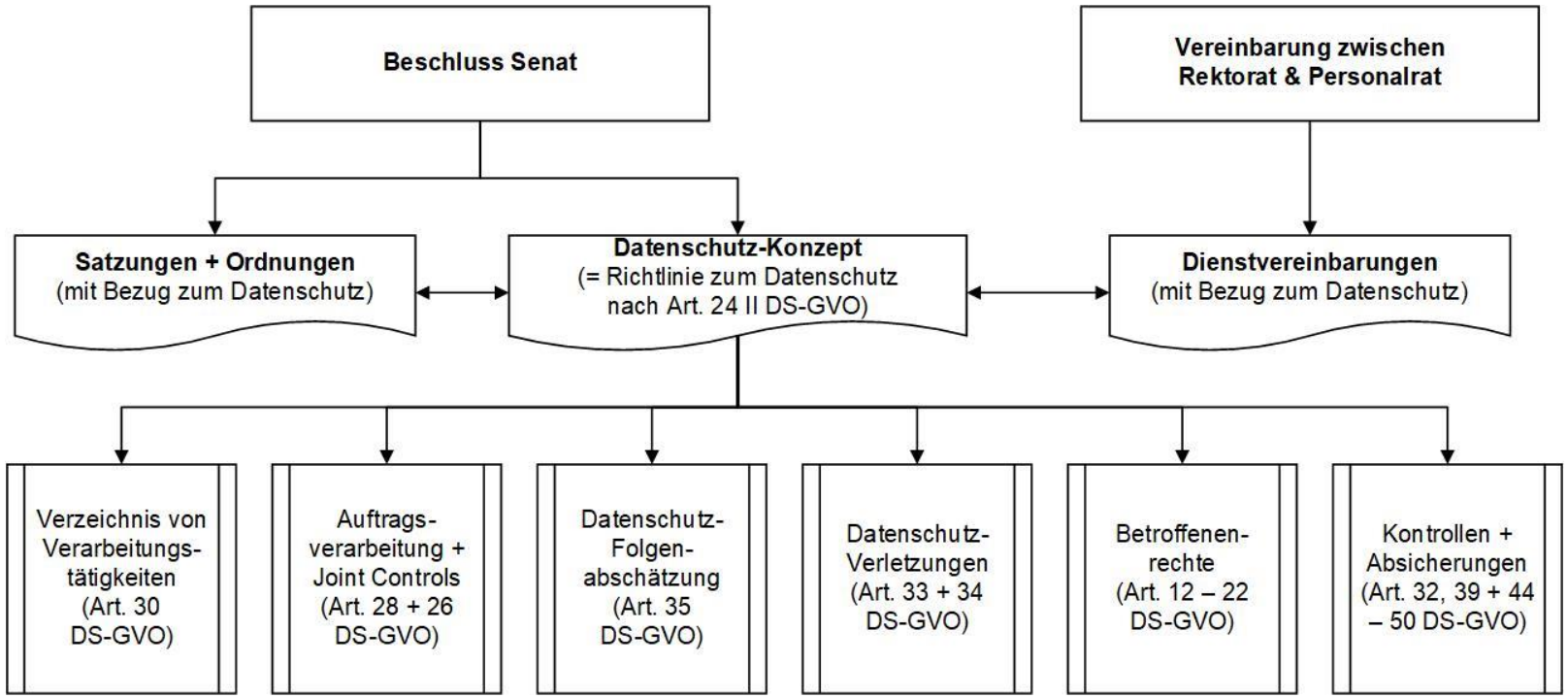
Aufgabe:

- Welche Prozesse hat eine Universität zum **Datenschutzmanagement** aufgrund der datenschutzrechtlichen Bestimmungen aus EU-DSGVO umzusetzen?
  Hinweis:
  Unter Prozesse sind festgelegte, handlungsanleitende Arbeitsschritte zu verstehen, welche sachlich miteinander zusammen hängen. Für das Management wiederum sind nur Steuerungsprozesse maßgeblich. Bei Universitäten betrifft dies Beschäftigten-Datenschutz, Datenschutz in der Lehre und Prüfungsverwaltung, Forschungs-Datenschutz und Datenschutz bei Veröffentlichungen und Drittmittelverwaltung. Listen Sie daher nur solche Prozesse auf, die bei der Erfüllung daten-schutzrechtlicher Vorschriften eine Steuerungswirkung haben.

2.2 Datenschutzmanagement II

Aufgabe:

- *Generell gilt:*



2.2 Datenschutzmanagement (1)

- Nach § 2 Abs. 1 Nr. 1 LHG obliegt den Universitäten die Pflege und Entwicklung der Wissenschaften in der Verbindung von
  - **Forschung**,
  - **Lehre**,
  - **Studium** und
  - **Weiterbildung**
- Nach § 2 Abs. 9 LHG **unterrichten** die Hochschulen die **Öffentlichkeit** regelmäßig **über** die Erfüllung ihrer Aufgaben und die dabei erzielten **Ergebnisse** → Veröffentlichungspflicht mit Personenbezug, da leicht auf Verantwortliche zuordnenbar
- Nach § 3 Abs. 2 LHG umfasst die **Freiheit der Forschung** insbesondere die Fragestellung, die Grundsätze der Methodik sowie die Bewertung des Forschungsergebnisses und seine Verbreitung. Nach § 3 Abs. 3 LHG umfasst die **Freiheit der Lehre** insbesondere die Abhaltung von Lehrveranstaltungen und deren inhaltliche und methodische Gestaltung sowie das Recht auf Äußerung von wissenschaftlichen Lehrmeinungen. → Individualrechte
- Nach § 5 Abs. 2 LHG nehmen die Hochschulen zur **Bewertung** der Erfüllung ihrer Aufgaben regelmäßig **Eigenevaluationen** vor. Die Ergebnisse sollen **veröffentlicht** werden. Nach § 5 Abs. 3 LHG dokumentieren die Hochschulen in pseudonymisierter oder anonymisierter Form Verlaufsdaten der Studien- und Qualifizierungsverläufe der Studierenden und des wissenschaftlichen Nachwuchses. [*Ergänzung: Nach § 13 Abs. 2 LDSG sind personenbezogenen Daten aus Forschungen zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist; § 27 Abs. 3 BDSG dagegen nur für besondere Kategorien*]

2.2 Datenschutzmanagement (2)

- Nach § 8 Abs. 5 LHG kann die Hochschule ihre Angelegenheiten durch sonstige **Satzungen** regeln, soweit die Gesetze keine Vorschriften enthalten.
- Nach § 12 Abs. 3 LHG regeln die Hochschulen die **Verarbeitung personenbezogener Daten**, insbesondere die Erhebung, Nutzung, Übertragung sowie die Aufbewahrungsdauer und Löschung durch **Satzung**.
- Nach § 13 Abs. 8 LHG richten die Hochschulen ein **Informationssystem** ein, das die Grunddaten der Ressourcenausstattung und -nutzung für die Leistungsprozesse der Lehre, der Forschung und bei den sonstigen Aufgaben der Hochschulen sowie der Erfüllung des Gleichstellungsauftrages enthalten muss. Zu den Grunddaten gehören insbesondere Angaben über die gegenwärtige Situation, die mehrjährige fachliche, strukturelle, personelle, bauliche und finanzielle Entwicklung und die Ergebnisse der Leistungsprozesse.
- Nach § 26 Abs. 1 BDSG dürfen **personenbezogene Daten von Beschäftigten** für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist [*Anmerkung: Für Universitäten gelten tatsächlich an dieser Stelle § 15 Abs. 1 LDSG; für diese Übungsaufgabe jedoch bewusst vereinfacht, da § 15 Abs. 4 LDSG wiederum für die Verarbeitung von Personalaktendaten auf §§ 83 – 88 LBG verweist*]

2.2 Datenschutzmanagement (3)

- Erlass geeigneter **Datenschutzrichtlinien** (nach Art. 24 Abs. 2 EU-DSGVO) & universitärer **Satzungen**, insbesondere zur Evaluierung nach § 5 Abs. 5 LHG und zur Verarbeitung personenbezogener Daten nach § 12 Abs. 3 LHG
  → Richtlinien und Satzung soweit sogar rechtsetzend für Universität!
- Durchführung vorgeschriebener **Datenschutz-Folgenabschätzungen** nach Art. 35 Abs. 1 EU-DSGVO bei Verwendung neuer Technologien, aufgrund Art, Umfang, Umstände und Zwecke der Verarbeitung mit hohem Risiko für die Rechte und Freiheiten natürlicher Personen, was für die Fälle aus Art. 35 Abs. 3 EU-DSGVO explizit zu erwarten ist
  → Ermittlung nötiger Schutzvorkehrungen zur Vermeidung hoher Risiken
- Festlegung geeigneter technischer & organisatorischer **Maßnahmen zur Sicherheit der Verarbeitung** nach Art. 32 EU-DSGVO, angemessen zum Schutzbedarf & nach Stand der Technik und deren regelmäßige Überprüfung & Aktualisierung (aufgrund von Art. 24 Abs. 1 EU-DSGVO)
  → Fortlaufende Aktualisierung getroffener Schutzvorkehrungen
- Durchführung der **Regelkontrolle** hinsichtlich der Einhaltung von Datenschutzvorschriften durch den Datenschutzbeauftragten nach Art. 39 Abs. 1 lit. b EU-DSGVO
  → Interne Überprüfung der Datenschutzkonformität
- Durchführung vorgeschriebener **Meldungen von Datenpannen** nach Art. 33 & 34 EU-DSGVO
  → Externe Kommunikation über Datenpannen
- Auswahl geeigneter **Auftragsverarbeiter** nach Art. 28 EU-DSGVO

2.3 Datenschutzerklärung

Aufgabe:

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

2.3 Datenschutzerklärung (1)

- Zur Online-Lehre an der Universität werden Vorlesungen und Übungen mittels Videokonferencing abgewickelt, welches vom <<Anbieter>> auf der Grundlage einer Datenschutzvereinbarung unter Einsatz eines Data Centers auf dem Gebiet der EU betrieben wird. Details zur Datenverarbeitung durch dieses Videokonferencing kann der zugehörigen Datenschutzerklärung auf <<Anbieter-Webseite>> entnommen werden.
- Dieses Videokonferencing 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 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.

2.3 Datenschutzerklärung (2)

- Bei Nutzung des Videokonferencing 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 Videokonferencing abgewickelte Online-Lehre wird defaultmäßig nicht und ansonsten nur mit Zustimmung aller Beteiligten aufgezeichnet.

2.3 Datenschutzerklärung (3)

- Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen der Nutzung der Videokonferencing 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 Nutzungsdaten interpersoneller Telekommunikationsdienste im Sinne von § 2 Abs. 2 Nr. 3 TTDSG und zugehörigen Verkehrsdaten.
  *Hinweis: Nach den **§§ 6 Abs. 2, 9 Abs. 2, 12 und 19 TTDSG** resultieren daraus **besondere Schutzvorkehrungen**.*
- Die Teilnehmenden einer Lehrveranstaltung, die mittels Videokonferencing 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.

2.4 Löschkonzept

Aufgabe:

- Entwerfen Sie unter Beachtung relevanter Vorschriften aus dem TTDSG 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.

2.4 Löschkonzept (1)

- Mailingliste ist ein interpersoneller Telekommunikationsdienst
  → Neben den allgemeinen Datenschutzvorschriften aus der EU-DSGVO treten insoweit Vorschriften aus dem TTDSG hinzu
  (aktueller Hinweis: Auf EU-Ebene steht derzeit noch 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
- Daten über Abonnenten sind Bestandsdaten (§ 2 Abs. 2 Nr. 2 TTDSG), Archivdaten Nutzungsdaten (§ 2 Abs. 2 Nr. 3 TTDSG) & das Archiv ein Dienst mit Zusatznutzen (§ 2 Abs. 2 Nr. 5 TTDSG)

2.4 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!

2.4 Löschkonzept (3)

- In der Einwilligungserklärung zum Abonnement der Mailingliste muss daher die Speicherung gesendeter Beiträge (= Verkehrsdaten mit Zusatznutzen!) und deren Ablage im Mailinglisten-Archiv von der abonnementsbezogenen Löschung im Sinne von § 9 Abs. 2 TTDSG 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, Anonymisierung stellt nach § 9 Abs. 2 TTDSG zulässige Umsetzung dar

2.4 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. 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
- Nach § 6 Abs. 2 TTDSG muss ein unbefugtes Offenbaren von Nachrichteninhalten nach Stand der Technik vermieden werden
- Aufgrund von § 19 Abs. 2 TTDSG ist in der Datenschutzerklärung über die Möglichkeit zur anonymen oder pseudonymen Nutzung hinzuweisen (→ Löschung von Identifikationsdaten aus Bestandsdaten für Archiv-Nutzer im Löschkonzept auszuführen)

2.4 Löschkonzept (5)

- Nach § 9 Abs. 1 TTDSG sind Nutzungsdaten zum Abruf von Archivdaten unverzüglich zu löschen → Teil des Löschkonzepts
- 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
- 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)

2.4 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)

2.5 Einwilligung in Web-Tracking I

Aufgabe:

- Ein Unternehmen möchte die Nutzung ihrer Webseite mittels eines Tracking-Tools analysieren, das die IP-Adressen der Nutzer und die getätigten Klicks sowie die eingegebenen Suchanfragen zu Analysezwecken an einen für derartige Analysen spezialisierten Dritten in einem Drittland ohne angemessenes Datenschutzniveau überträgt. Zu diesem Zweck soll auf dem Endgerät des Nutzers ein Cookie gespeichert werden. Der bereitgestellte Telemediendienst soll eine pseudonyme Nutzung ermöglichen. Formulieren Sie eine geeignete **elektronische Einwilligungserklärung** zur Speicherung des zugehörigen Cookies!

2.5 Einwilligung in Web-Tracking II

Aufgabe:

- *<u>Hinweis:</u>*
  Ziel von Tracking Tools ist die bedarfsgerechte Gestaltung angebotener Telemedien. Das Endgerät wird im TTDSG Endeinrichtung genannt. Das Setzen des Cookies ist nicht erforderlich, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.
  Gehen Sie in Ihrer Antwort davon aus, dass IP-Adressen als personenbezogenes Datum anzusehen sind, selbst wenn diese dynamisch erzeugt werden.

2.5 Einwilligung in Web-Tracking (1)

- *IP-Adressen werden nach herrschender Meinung als personenbezogene Daten angesehen, da Online-Kennung (siehe ErwG 30 und das Beispiel 15 zu dynamischen IP-Adressen in WP 136 der EU-Datenschutzgruppe nach Art. 29 EU-DSRL (Vorläufer des Europäischen Datenschutzausschusses)*
- *Aufgabe von Tracking-Tools ist es, das Verhalten der Web-Seiten-Nutzer hinsichtlich deren Klicks und Eingaben auf den bereitgestellten Web-Seiten zu analysieren und daraus Rückschlüsse zur Verbesserung des eigenen Web-Auftritts bzw. der dort angebotenen Produkte / Leistungen ziehen zu können*
  - *→ Ziel: bedarfsgerechte Gestaltung angebotener OTT-Dienste!*
  - *→ Einwilligung nach § 9 Abs. 2 TTDSG nötig!*
  - *→ Wegen Datenübertragung in Drittland Art. 49 Abs.1 lit. a EU-DSGVO bei Einwilligung berücksichtigen!*
  - *→ Da Cookie auf Endeinrichtung des Nutzers gespeichert wird, muss Einwilligung zudem § 25 Abs. 1 TTDSG erfüllen!*
  - *→* ***Cookie darf erst nach Einwilligung gesetzt werden****!*

2.5 Einwilligung in Web-Tracking (2)

Hiermit willige ich ein, dass die gespeicherte IP-Adresse, meine Klicks sowie von mir eingegebene Suchanfragen zum Zweck der bedarfsgerechten Gestaltung der Webseite von der <Bezeichnung des Verantwortlichen> unter Berücksichtigung der zugesicherten pseudonymen Nutzung verwendet werden dürfen. Ich bin damit einverstanden, dass die Analysen durch einen spezialisierten Dritten in einem Drittland ohne angemessenes Datenschutzniveau durchgeführt werden. Ich wurde darüber informiert, dass ich diese Einwilligung jederzeit ohne Nachteile widerrufen kann. Mir ist bewusst, dass aus Gründen der Nachvollziehbarkeit der Vorgang der Einwilligung selbst mitprotokolliert wird. Von der <Bezeichnung des Verantwortlichen> wurde mir versichert, dass meine datenschutzrechtlichen Belange ohne Einschränkung gewährleistet werden.

☐ Obiger Einwilligungserklärung stimme ich zu! *(bitte Häkchen setzen)*

☒ *Absenden!*