Grundlagen des Datenschutzes und der IT-Sicherheit

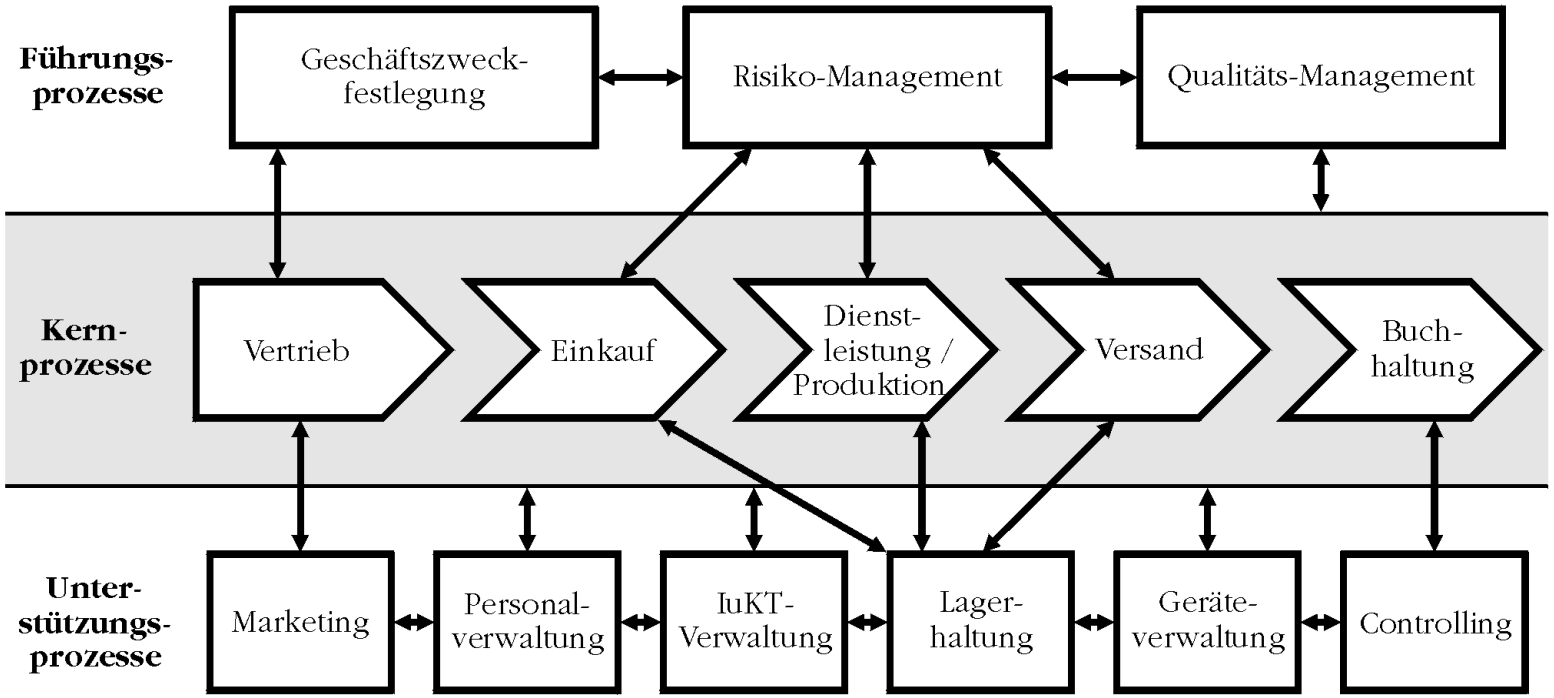
Musterlösung zur 2. Übung im SoSe 2025:

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 Verarbeitung personenbezogener
  a) Kundendaten
  b) Beschäftigtendaten

2.1 Verfahren

a) Kundendaten-verarbeitung

Marketing:

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

Vertrieb:

- Vertragsabwicklung
- Customer Relationship Management

Buchhaltung:

- Zahlungsüberwachung

Versand:

- Versand

IuKT-Verwaltung:

- Elektronische Kommunikation

b) Beschäftigtendaten-verarbeitung

Personalverwaltung:

- Bewerbungsverfahren
- Personalaktenführung
- Arbeitszeitüberwachung

Buchhaltung:

- Lohn- und Gehaltsabrechnung

Dienstleistung / Produktion:

- Betriebsdatenerfassung

Qualitäts-Management:

- Qualitätskontrolle

Controlling:

- Leistungskontrolle

IuKT-Verwaltung:

- Elektronische Kommunikation

2.2 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!

2.2 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.

2.2 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.

2.2 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 TDDDG und zugehörigen Verkehrsdaten.
  *Hinweis: Nach den **§§ 6 Abs. 2, 9 Abs. 2, 12 und 19 TDDDG** 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.

2.2 Datenschutzerklärung (4)

Zum Spezialfall (nach Blitzumfrage): **Soziales Netzwerk als digitaler Dienst**

- Soziales Netzwerk ist ein Online-Dienst mit Zusatznutzen im Sinne von § 2 Abs. 2 Nr. 5 TDDDG. Hierbei stellt der Betreiber des Sozialen Netzwerks „nur“ die Plattform für die Veröffentlichung und dauerhaften Speicherung von Content (soweit Basisdienst) und zusätzliche Funktionen zur Verknüpfung zwischen Nutzern sowie Auffinden spezifischen Contents (soweit Zusatznutzen).
- Datenschutzrechtlich ist der Betrieb einer eigenen Content-Seite (sog. „Fanpage“) auf einem Sozialen Netzwerk als **Joint Controllership** nach Art. 26 EU-DSGVO. Darauf muss in der Datenschutzerklärung hingewiesen werden.
- Werden auf der „Fanpage“ selbst personenbezogene Daten von Nutzern oder Dritten erhoben, gespeichert und ggf. für weitergehende Zwecke (z.B. Werbung) weiterverarbeitet, muss folglich auf alle Zwecke in der eigenen Datenschutzerklärung des „Fanpage“-Betreibers hingewiesen werden. In der Regel wird hier auf Art. 6 Abs. 1 lit. f EU-DSGVO abgestellt (berechtigtes Interesse), doch ist hier für den Zusatznutzen aufgrund von § 9 Abs. 2 TDDDG eine Einwilligung nötig. Die Datenschutzerklärung muss dabei von der betreffenden „Fanpage“ aus direkt aufrufbar sein.
- Da Soziale Netzwerke überwiegend aus Ländern ohne angemessenes Datenschutzniveau betrieben, ist darauf explizit hinzuweisen (siehe auch 2.4).

2.3 Löschkonzept

Aufgabe:

- Entwerfen Sie unter Beachtung relevanter Vorschriften aus dem TDDDG 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 im Sinne eines bereitgestellten Dienstes mit Zusatznutzen zugänglich ist! Berücksichtigen Sie dabei auch, wie mit Datensicherungen umzugehen ist.

2.3 Löschkonzept (1)

- Mailingliste ist ein interpersoneller Telekommunikationsdienst → Neben den allgemeinen Datenschutzvorschriften aus der EU-DSGVO treten insoweit Vorschriften aus dem TDDDG hinzu
- 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 TDDDG), Archivdaten Nutzungsdaten (§ 2 Abs. 2 Nr. 3 TDDDG) & das Archiv ein Dienst mit Zusatznutzen (§ 2 Abs. 2 Nr. 5 TDDDG)

2.3 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!

2.3 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 TDDDG 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 TDDDG zulässige Umsetzung dar

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

2.3 Löschkonzept (5)

- Nach § 9 Abs. 1 TDDDG 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)

2.3 Löschkonzept (6)

- Nach § 35 Abs. 1 BDSG 2024 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)

2.4 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 Analyse-zwecken 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 Telekommuni¬kationsdienst soll eine pseudonyme Nutzung ermöglichen. Formulieren Sie eine geeignete **elektronische Einwilligungserklärung** zur Speicherung des zugehörigen Cookies!

2.4 Einwilligung in Web-Tracking II

Aufgabe:

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

2.4 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 TDDDG 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 TDDDG erfüllen!*
  - *→* ***Cookie darf erst nach Einwilligung gesetzt werden****!*

2.4 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!*

2.5 Messenger Dienst

Aufgabe:

- Ein Unternehmen möchte für seine Beschäftigten die Nutzung eines **Messenger Dienstes** erlauben, über welches dienstliche Mitteilungen versendet und empfangen werden dürfen. Wie muss es dazu vorgehen, dass relevante **Anforderungen aus dem Datenschutz und des Schutzes vertraulicher Kommunikation** dabei eingehalten werden?

2.5 Messenger Dienst (1)

- Messenger Dienste sind sog. „Over-the-top-Dienste“ (interpersoneller Kommunikationsdienst nach § 3 Nr. 24 TKG zum Austausch von Nachrichten zwischen einem Sender und n Empfängern)
- Wenn also ein Messenger Dienst nur für dienstliche Zwecke eingesetzt werden soll, ist entscheidend, dass nur Empfänger als Nachrichtenempfänger eingetragen werden, die dienstlich dafür vorgesehen sind; ist das auf das spezifische Unternehmen beschränkt, lässt sich dieses technisch einschränken, andernfalls nur organisatorisch
- Die Inhalte der Nachrichten als auch der Umstand, wer mit wem Nachrichten austauscht, unterliegt jedoch dem Fernmeldegeheimnis nach § 3 Abs. 1 TDDDG

2.5 Messenger Dienst (2)

- Nach § 6 Abs. 2 TDDDG sind Fehlübermittlungen und das unbefugte Offenbaren von Nachrichteninhalten innerhalb des Unternehmens des Anbieters und an Dritte auszuschließen
  → Nachrichteninhalte dürfen nur durch Befugte eingesehen werden
  → Für die vorgesehenen Zwecke ist festzulegen, wer als befugt anzusehen ist
  → Messenger Dienst bevorzugt On-Premise betreiben oder Ende-zu-Ende verschlüsseln
- Nach § 9 Abs. 2 TDDDG dürfen Verkehrsdaten nur zur Bereitstellung von Diensten mit Zusatznutzen weiter gespeichert werden
  → Dienst mit Zusatznutzen ist explizit festzulegen, mit dem eine Zeitspanne über das reine unmittelbare Kommunikation (z.B. zu benötigten Nachweiszwecken) begründet wird
  → Nach Ablauf dieser Zeitspanne sind die Daten automatisiert zu löschen

2.5 Messenger Dienst (3)

- Zudem bedarf der Einsatz des Messenger Dienstes einer **Datenschutzerklärung** nach Art. 13 EU-DSGVO
- Wenn der Messenger Dienst ausschließlich für dienstliche Belange eingesetzt werden darf und der Austausch entsprechender Textnachrichten zugleich für die Aufgabenerfüllung erforderlich ist, kommt möglicherweise Art. 6 Abs. 1 lit. b EU-DSGVO als **Rechtsgrundlage** in Frage (Beschäftigter ist hier vermittels seines Anstellungsvertrags Vertragspartei!), sonst (der wahrscheinlichere Fall) Art. 6 Abs. 1 lit. f EU-DSGVO unter Angabe, welche berechtigten Interessen dabei zum Tragen kommen – vom Konstrukt auf Basis von Einwilligungserklärung ist dagegen dringend abzuraten, da technisch nicht komfortabel umsetzbar.
- Bei der Rechtsgrundlage nach Art. 6 Abs. 1 lit. b EU-DSGVO besteht u.U. jedoch die Erfordernis, die Chatnachristen aus Gründen der Gewährleistung i.d.R. 2 Jahre aufzubewahren.