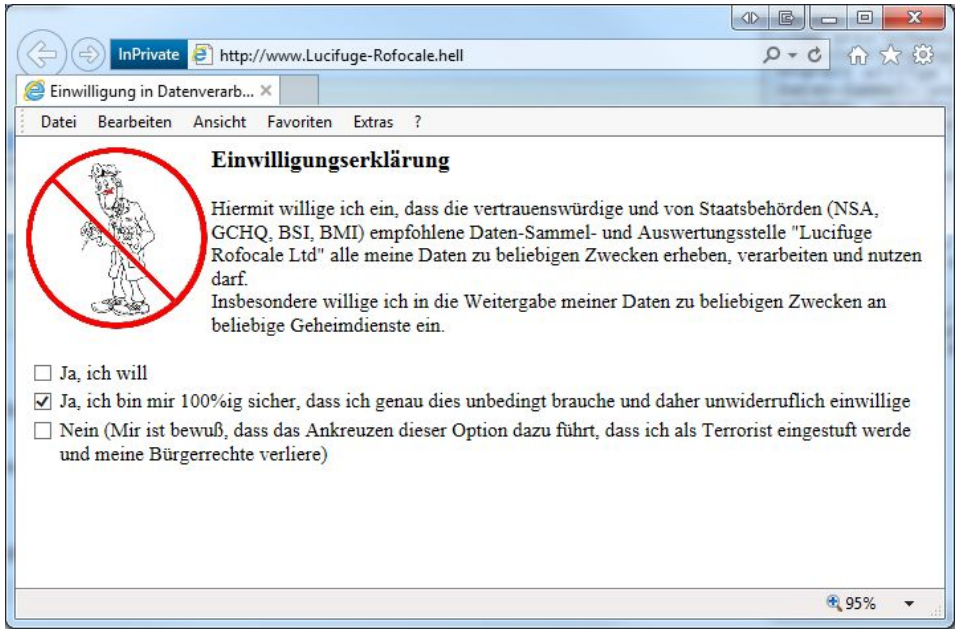

BETROFFENENRECHTE

Dr. Bernd Schütze

Seminar Datenschutz-Grundverordnung (DS-GVO)

HEALTHCARE SOLUTIONS

Agenda

Was gehört alles dazu?

- Transparenzpflichten
- Informationspflichten
- Auskunftsrecht
- Berichtigung
- Löschung / Einschränkung der Verarbeitung
- Datenübertragbarkeit
- Widerspruchsrecht
- Automatisierte Einzelfallentscheidung

Transparenzpflichten

Art. 12: Anforderungen an die Transparenz

Art. 12: Anforderungen

Informationen müssen

- präziser,
- transparenter,
- verständlicher und
- leicht zugänglicher Form in einer
- klaren und einfachen Sprache
- gegeben werden

Keine Legaldefinition;

Wie EU-weit auszulegen?

Art. 12: Anforderungen an die Transparenz

Beispiel: einfache Sprache

- Verwendung von Wörtern der Alltagssprache
- Fremdwörter müssen erklärt werden
- Ziel: alle Menschen verstehen den Inhalt, insbesondere auch
  - Menschen, die eine andere Muttersprache als Deutsch haben
  - Menschen, die nicht so gut Deutsch sprechen
  - Menschen mit und ohne Behinderung, insbesondere auch Menschen mit einer Hör-Behinderung

Quelle: Büro für Leichte Sprache Bonn, https://www.leichte-sprache-bonn.de/einfache-sprache/

Art. 12: Anforderungen an die Transparenz

Beispiel: klare Sprache

- Leicht verständlich = jeder kann sie verstehen
- Korrektes, aber einfaches Deutsch
- Verwendung von Fremdwörtern nur dort, wo es notwendig ist
- Fach-Wörter, die notwendig sind, werden erklärt; danach durchgängig im Text genutzt

Quelle: Touchdown 21, http://www.touchdown21.info/de/seite/7-ueber-uns/article/163-was-ist-klare-sprache.html

Art. 12: Anforderungen an die Transparenz

Klar und deutlich schreiben

- Europaweit einheitliche Auslegung erforderlich
- Daher als Orientierungshilfe
- EU Veröffentlichung „Klar und deutlich schreiben“ https://publications.europa.eu/de/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5

Art. 12: Anforderungen an die Transparenz

Formvorgaben

- Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, ggf. auch elektronisch
  - ErwGr: 58

    „Diese Information könnte in elektronischer Form bereitgestellt werden, beispielsweise auf einer Website, wenn sie für die Öffentlichkeit bestimmt ist.
    Dies gilt insbesondere für Situationen, wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik [...]“
- Wenn von Person verlangt und Identität nachgewiesen wurde, kann Information mündlich gegeben werden
- Alle Informationen der Artt. 13-22 und Art. 34 werden unentgeltlich zur Verfügung gestellt (Art. 12 Abs. 5)
  - Unbegründete und exzessive Anträge erlauben Berechnung der Verwaltungskosten
  - Nachweispflicht bzgl. unbegründet/exzessiv: Verantwortlicher
- Identität betroffene Person muss gewährleistet sein
  - Begründete Zweifel an Identität -> Anforderungen zusätzlicher Informationen zum Nachweis der Identität

Art. 12: Anforderungen an die Transparenz

Standardisierte Bildvorgaben

- Informationen aus Artt. 13,14 können durch standardisierte Bildsymbole bereitgestellt werden
- EU-Kommission: delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, erlassen (Art. 12 Abs. 8)
- Desgleichen Verfahren für die Bereitstellung der Bildsymbole (Art. 12 Abs. 8)

→ Merke:

  → Es dürfen nur Bildsymbole verwendet werden, die seitens der EU-Kommission erlassen wurden

  → Bildsymbole dürfen nur in von der EU-Kommission definierten Verfahren genutzt werden

→ „Eigenentwicklung“ entspricht nicht den gesetzlichen Vorgaben

Art. 12: Anforderungen an die Transparenz Standardisierte Bildvorgaben

DS-GVO Parlamentsversion, Anhang Darstellung durch Symbole*

Es werden nicht mehr pbD **erhoben**, als für die spezifischen Zwecke der Verarbeitung erforderlich sind

PbD werden nicht zu anderen Zwecken **verarbeitet**, für die sie erhoben wurden

Es werden keine pbD an gewerbliche Dritte **weitergegeben**

Es werden keine pbD **unverschlüsselt** aufbewahrt

Es werden keine pbD **verkauft** oder **verpachtet**

Wer hat was erkannt?

* Parlamentsversion vom 12. März 2014: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP// TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE

Art. 12: Anforderungen an die Transparenz
Standardisierte Bildvorgaben

Netzpolitik.org: „Iconset für Datenschutzerklärungen“*

Real Name / Adress

Mailadress

Mails, Messages

for Friends, Contacts

end of usage / logout

Wer hat was erkannt?

* https://netzpolitik.org/2007/iconset-fuer-datenschutzerklaerungen/

Informationspflichten

Informationspflichten

Wie werden Daten erhoben?

- Personenbezogene Daten können
  - Bei der Person direkt erhoben werden („Direkterhebung“)
    - Hinweis: Direkterhebung dt. Recht* = jede Erhebung pbD mit Kenntnis oder unter Mitwirkung der betroffenen Person
  - Mittelbar über Dritte erhoben werden
- Direkterhebung
  - Zum Zeitpunkt der Erhebung umfassend informieren (Art. 13)
  - Hinweis: unter DS-GVO Grundsatz der Direkterhebung nicht mehr gegeben
- Erhebung über Dritte
  - Innerhalb einer angemessenen Frist nach Erlangung der Daten informieren, längstens innerhalb eines Monats (Art. 14)
  - Bei Nutzung der Daten zur Kommunikation mit Betroffenen: spätestens zum Zeitpunkt der ersten Mitteilung

Informationspflichten

Welche Angaben sind erforderlich?

- Name und Kontaktdaten des Verantwortlichen
- Ggf. Kontaktdaten Datenschutzbeauftragter
- Zwecke der Verarbeitung
- Rechtsgrundlage
  - Information, ob Bereitstellung gesetzlich oder vertraglich vorgeschrieben ist
  - Information, welche (möglichen) Folgen Nicht-Bereitstellung hat
- Kategorien der Daten
- Empfänger der Daten (ggf. auch Kategorien von Empfängern
- (Absicht) Übermittlung in Drittland
- Speicherdauer
- Hinweis auf Bestehen einer automatisierten Einzelfallentscheidung (Art. 22)
- Bei Erhebung von einem Dritten: Angabe der Quelle der Daten
- Ggf. Information bzgl. (beabsichtigter) Zweckänderung

Informationspflichten

Ebenfalls verpflichtend: Hinweis auf Betroffenenrechte

- Recht auf Auskunft (Art. 15)
- Recht auf Berichtigung (Art. 16)
- Recht auf Löschung (Art. 17)
- Recht auf Einschränkung (Art. 18)
- Recht auf Datenübertragbarkeit (Art. 20)
- Recht auf Widerspruch (Art. 21)
  - Cave: „in einer von anderen Informationen getrennten Form“ (Art. 21 Abs. 4)
- Recht auf Widerruf einer Einwilligung (Art. 7)
- Recht auf Beschwerde bei einer Aufsichtsbehörde

Informationspflichten

Unterschiede bei Direkterhebung und Dritterhebung

- Die Pflichten unterscheiden sich bzgl. Art. 13 und Art. 14 nicht grundsätzlich, aber
- Informationspflichten entsprechend der Abs. 2 nicht absolut:
  - [...] die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten
- Informationen sind nicht immer mitzuteilen, nur bei Notwendigkeit
  - Aber: Nachweispflicht aus Art. 5 = nicht vorhandene Notwendigkeit dokumentieren und nachweisen können

Informationspflichten: Was fordert Art. 13, was Art. 14 DS-GVO?

Informationspflicht	Art. 13	Art. 14
Kontaktdaten Verantwortlicher	Abs. 1	Abs. 1
Kontaktdaten Datenschutzbeauftragter	Abs. 1	Abs. 1
Zwecke Verarbeitung	Abs. 1	Abs. 1
Rechtsgrundlage Verarbeitung	Abs. 1	Abs. 1
Kategorien der Daten	-	Abs. 1
Empfänger der Daten	Abs. 1	Abs. 1
Drittstaatentransfer	Abs. 1	Abs. 1
Speicherdauer	Abs. 2	Abs. 2
Information bzgl. Betroffenenrechte	Abs. 2	Abs. 2
Widerruf Einwilligung	Abs. 2	Abs. 2
Einzelfallentscheidung	Abs. 2	Abs. 2
Angabe Quelle	-	Abs. 2

BDSG n.F.

Bei Direkterhebung gilt national

- Keine Informationspflicht besteht
  - Weiterverarbeitung analog gespeicherter Daten betrifft, wenn
    - Verantwortliche sich durch die Weiterverarbeitung unmittelbar an die betroffene Person wendet
    - Zweck mit dem ursprünglichen Erhebungszweck vereinbar ist
    - Kommunikation mit der betroffenen Person nicht in digitaler Form erfolgt
    - Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls als gering anzusehen ist
  - Verarbeitung einer öffentlichen Stelle und Interessensabwägung ergibt, Interesse der öffentlichen Stelle überwiegt
  - Information gefährdet öffentliche Sicherheit/Ordnung
  - Information bereitet dem „Wohl des Bundes oder eines Landes“ Nachteile
  - Die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche wird durch Information behindert
  - Die Interessen des Verantwortlichen an der Nichterteilung der Information überwiegen die Interessen der betroffenen Person

BDSG n.F.

Bei Direkterhebung gilt national

- Bei Unterlassen der Information:
  - Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Personen müssen ergriffen werden
  - Bereitstellung der Informationen entspr. Art. 13 Abs. 1,2 Ds-GVO für die Öffentlichkeit
  - Schriftlich festhalten, aus welchen Gründen Information Betroffener nicht erfolgte
- Bei Vorübergehendem Hinderungsgrund: Information muss nach Fortfall Hinderungsgrund nachgeholt werden

BDSG n.F.

Erhebung über Dritte

- Keine Informationspflicht besteht für nicht-öffentliche Stelle
  - Information beeinträchtigt Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche
  - Zuständige öffentliche Stelle stellte gegenüber dem Verantwortlichen fest, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährdet oder dem Wohl des Bundes oder eines Landes Nachteile bereitet
  - Datenverarbeitung erfolgt für Zwecke der Strafverfolgung
- Bei Unterlassen der Information:
  - Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Personen müssen ergriffen werden
  - Bereitstellung der Informationen entspr. Art. 13 Abs. 1,2 DS-GVO für die Öffentlichkeit
  - Schriftlich festhalten, aus welchen gründen Information Betroffener nicht erfolgte

Informationspflichten

Fazit

- Informationspflichten müssen eine faire und transparente Verarbeitung ermöglichen
- In diesem Sinne müssen sie interpretiert und gelebt werden
- Fragen, die man sich stellen muss
  - Was muss der Betroffene wissen?
  - Was will der Betroffene wissen?
  - Kann der Betroffene die Informationen verstehen, die ich ihm anbiete?

Beispiel: Datenschutzhinweise auf Internetseiten

Webseiten müssen über Erhebung informieren

- Verantwortliche(r)
- Begriffsbestimmungen
- Betroffenenrechte
- Datenweitergabe
- Ort der Datenverarbeitung
- Daten bzw. Datenkategorien
- Verwendungszweck
- Speicherdauer
- Weitere Verantwortliche (im Rahmen der Weitergabe)

Auskunftsrecht

Recht aus Auskunft

Grundsätzliches

- Gegenüber bisheriges BDSG ähnlich, aber weitergehende Auskunftspflicht
- Auskunft = Identität einer Auskunft suchenden betroffenen Person ist gewährleistet (ErwGr. 64)
- Auskunft muss für betroffene Person „problemlos und in angemessenen Abständen“ nutzbar sein (ErwGr. 63)
- Auskunft soll betroffener Person (auch) dazu dienen, die Rechtmäßigkeit der Verarbeitung zu prüfen (ErwGr. 63)
- Nach Möglichkeit soll „Fernzugang zu einem sicheren System“ zum Zugang der Informationen für betroffene Personen zur Verfügung gestellt werden (ErwGr. 63)

Recht aus Auskunft

Grundsätzliches

- Auskunftserteilung innerhalb von 4 Wochen
  - Terminüberschreitung
  - Fristverlängerung: um zwei Monate, falls aufgrund Komplexität und Anzahl der Anträge erforderlich
  - Begründete Information bzgl. Fristverlängerung an die betroffene Person innerhalb des ersten Monats erforderlich
- Form der Auskunft
  - Bei elektronischer Anfrage: Auskunftserteilung in einem gängigen elektronischen Format, falls betroffene Person nichts anderes angibt
  - Auskunftserteilung ohne Beeinträchtigung der Rechte und Freiheiten anderer Personen
- Recht auf Kopie für betroffen Person
  - Erste Kopie kostenlos, weitere Kopien Berechnung Verwaltungskosten erlaubt
  - Antrag elektronisch: Informationen sind in „gängigen elektronischen Format“ zur Verfügung zu stellen (außer Person gibt anderes an)

Recht aus Auskunft

Auskunft beinhaltet mindestens...

- Verarbeitungszwecke
- Kategorien personenbezogener Daten
- Empfänger oder Kategorien von Empfängern
- Ggf. Drittlandtransfer
- Speicherdauer
  - Falls nicht möglich: Kriterien für die Festlegung dieser Dauer
- Hinweis auf Betroffenenrechte (Berichtigung, Löschung, Einschränkung Verarbeitung, Widerspruchsrecht gegen Verarbeitung)
- Hinweis auf Beschwerderecht bei Aufsichtsbehörde
- Quelle der Daten (keine Pflicht bei Direkterhebung)
- Automatisierte Entscheidungsfindung
  - „Aussagekräftige Informationen“ bzgl. Ergebnisfindung
  - Tragweite/Auswirkungen für betroffene Person
- Drittlandtransfer: Darlegung der geeigneten Garantien gemäß Artikel 46

Recht aus Auskunft

Bsp. ErwGr. 63

- Recht betroffene Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten, etwa Daten in ihren Patientenakten
- Informationen wie beispielsweise
  - Diagnosen,
  - Untersuchungsergebnisse,
  - Befunde der behandelnden Ärzte und
  - Angaben zu Behandlungen oder Eingriffen

BDSG n.F.

Einschränkung des Rechts

Recht auf Auskunft besteht nicht

- Informationspflicht besteht entspr. §3 3 Abs. 1 Nr. 1 sowie Nr. 2 lit. b und Abs. 3 nicht
  - Abs. 1 betrifft nur öffentliche Stelle
  - Abs. 3 Verfassungsschutzbehörden, Bundesnachrichtendienst, Militärischen Abschirmdienst und bei Gefährdung der Sicherheit des Bundes andere Behörden des Bundesministeriums der Verteidigung, ist
- oder
  - Daten werden nur gespeichert, weil gesetzliche oder satzungsmäßige Aufbewahrungsvorschriften ein Löschen verbieten
  - Die Daten dienen ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle
  - Voraussetzung für Ausnahme:
    - Auskunftserteilung erfordert unverhältnismäßigen Aufwand und
    - Verarbeitung zu anderen Zwecken ist durch technische und organisatorische Maßnahmen ausgeschlossen

BDSG n.F.

Einschränkung des Rechts

- Gründe der Auskunftsverweigerung sind zu dokumentieren
- Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen
  - Außer: Mitteilung der Gründe gefährdet den mit der Auskunftsverweigerung verfolgten Zweck

Berichtigung

Berichtigung

Falsche/Fehlerhafte Daten müssen korrigiert werden

- Recht vom Verantwortlichen die unverzügliche Berichtigung sie betreffender unrichtiger personenbezogener Daten (Art. 16)
- Recht vom Verantwortlichen die Vervollständigung unvollständiger personenbezogener Daten - auch mittels einer ergänzenden Erklärung – zu verlangen (Art. 16)
- Art. 5 Abs. 1 lit. d: 1.Personenbezogene Daten müssen
  - sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden ("Richtigkeit");

Berichtigung

Fazit

- Verantwortlicher hat Pflicht, nur „richtige“ Daten zu speichern
- „Unrichtige“ Daten müssen korrigiert oder gelöscht werden
- Betroffener hat Recht
  - Unrichtige Daten korrigieren zu lassen
  - Ggf. ergänzende Informationen abspeichern zu lassen

  → Frage: Kann Ihr Informationssystem dies ggf. leisten? Von betroffener Person gegebene Erklärungen kontextbezogen ergänzend zur Information speichern?

Sperrung

Einschränkung der Verarbeitung

Grundsätzlich

Recht, Einschränkung der Verarbeitung zu verlangen, wenn

- Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird
  - Dauer der Sperrung: Notwendige Zeitdauer zur Überprüfung der Richtigkeit der Daten
- Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt
- Verantwortliche bedarf Daten für die Verarbeitungszwecke nicht länger, benötigt Daten aber zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- Person legte Widerspruch gegen die Verarbeitung ein (Art. 21)
  - Dauer der Sperrung: Notwendige Zeitdauer zur Überprüfung ob die berechtigten Gründe des Verantwortlichen zur Verarbeitung gegenüber denen der betroffenen Person überwiegen

Einschränkung der Verarbeitung

„Nebenpflichten“

- Verarbeitung (abgesehen von Speicherung) nur noch
  - mit Einwilligung der betroffenen Person oder
  - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder
  - zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder
  - aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaates
- Betroffen Person wird informiert, bevor die Einschränkung der Verarbeitung aufgehoben wird
- Allen Empfängern wird die Einschränkung mitgeteilt (Art. 19), außer
  - dies ist unmöglich oder
  - mit einem unverhältnismäßigen Aufwand verbunden

Einschränkung der Verarbeitung

ErwGR. 67

- Methoden können u.a. darin bestehen
  - ausgewählte personenbezogenen Daten vorübergehend auf ein anderes Verarbeitungssystem zu übertragen
  - die Daten für Nutzer zu sperren
  - veröffentliche Daten vorübergehend von einer Website zu entfernen
- Bei automatisierter Verarbeitung
  - Einschränkung grundsätzlich durch grundsätzlich durch technische Mittel, so dass Daten in keiner Weise weiterverarbeitet oder geändert werden können
  - Auf die Tatsache der Einschränkung wird in dem System unmissverständlich hingewiesen

BDSG n.F.

Ausnahmeregelung

- Bei nicht automatisierter Datenverarbeitung
  - Löschen wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und
  - Interesse der betroffenen Person an Löschung gering
  - → Löschen nicht erforderlich
- Löschen ist nicht erforderlich, wenn einer Löschung satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen

Löschung

Recht auf Löschung

Grundsätzlich

Betroffene Person hat Recht auf unverzügliche Löschung, wenn

- Daten sind für die Zwecke, für die sie verarbeitet wurden, nicht mehr notwendig
- Betroffene Person widerruft Einwilligung zur Datenverarbeitung, andere Rechtsgrundlage existiert nicht
- Person legt Widerspruch gegen Verarbeitung (Art. 21) ein und es liegen keine vorrangigen Gründe für die Verarbeitung vor
- Personenbezogene Daten werden unrechtmäßig verarbeitet
- Löschung ist zur Erfüllung einer gesetzlichen Pflicht, die der Verantwortliche unterliegt, erforderlich
- Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft erhoben

Recht auf Löschung

Aber...

Recht wird nur eingeschränkt

- Daten werden zur Ausübung des Rechts auf freie Meinungsäußerung und Information verarbeitet
- Daten werden zur Erfüllung einer rechtlichen Verpflichtung, die der Verantwortliche unterliegt, verarbeitet
- Daten werden zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, verarbeitet
- Daten werden aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit verarbeitet
- Daten werden für
  - im öffentlichen Interesse liegende Archivzwecke,
  - wissenschaftliche oder historische Forschungszwecke oder
  - für statistische Zwecke

  verarbeitet
- Daten werden zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen verarbeitet

Recht auf Löschung

„Nebenpflichten“

- Art. 17 Abs. 2

  Hat Verantwortlicher Daten „öffentlich“ gemacht und es besteht Löschpflicht,

  - so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art
  - um (andere) Verantwortliche bzgl. Löschpflicht aller Kopien, Replikationen usw. zu informieren
- Art. 19
  - Allen Empfängern wird die Löschung mitgeteilt
  - außer, dies ist unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden
- Auf Verlangen der betroffenen Person wird diese über alle Empfänger unterrichtet (Art. 19)

Also nur Löschen auf verlangen?

Keine Löschpflicht mehr unter der DS-GVO?

- Art. 5 Abs. 1 lit. e DS-GVO: 1.Personenbezogene Daten müssen
  - in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist [...]

→ Ohne Identifikationsmöglichkeit = Anonyme Daten = keine personenbezogene Daten

→ Löschen gefordert

BDSG n.F.

Keine Löschpflicht mehr unter der DS-GVO?

– §35 BDSG n.F.

1. Ist eine Löschung im Falle **nicht automatisierter Datenverarbeitung** wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten gemäß Artikel 17 Absatz 1 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679. Die Sätze 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

→ Papierakten müssen evtl. nicht gelöscht werden

→ Keine Ausnahmen für elektronische Datenverarbeitung

→ Absolute Löschpflicht

Löschen

Was heißt „Löschen“?

- Vier Möglichkeiten
  1. Entfernen der Signale

     Daten werden hierbei durch Entfernung (oder Überschreibung) der die Daten speichernden Signale gelöscht, ohne dass hierbei jedoch die Integrität des Datenträgers selbst beeinträchtigt wird
  2. Zerstörung des Datenträgers

     Daten werden durch das physikalische Zerstören des Datenträgers vernichtet und sind damit unkenntlich
  3. Löschung der Verknüpfung

     Ergibt sich eine zu löschende Information aus der Verknüpfung 2er (oder mehrerer) Teilmengen, jedoch nicht aus den unverknüpften Teilmengen, so kann eine datenschutzrechtliche Löschung der Information auch durch eine irreversible Löschung der Verknüpfung erfolgen.
  4. Fehlende Interpretierbarkeit

     Darstellende Zeichen sind i.S. bestimmter bedeutungshaltiger Aussagen nicht mehr interpretierbar

→ Fazit: **irreversible** Vernichtung der identifizierenden Daten = Löschung

→ Bisherige Interpretation „Löschen“ aus BDSG dürfte auch Anforderung aus Art. 5 DS-GVO genügen

Dammann: §3 BDSG, RN. 177-180. in: Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage, 2014. Nomos Verlagsgesellschaft. ISBN 978-3-8487-0593-1

Problemstellung: Heterogene Speicherorte

Patientendaten nicht an einem Ort gespeichert

- Patientendaten sind nicht in einem Informationssystem gespeichert, sondern in mehreren, z.B .
  - Krankenhaus-Informationssystem (KIS
  - Labor-Informationssystem (LIS)
  - Onkologisches Informationssystem (OIS)
  - Picture Archiving and Communication System (PACS)
  - Radiologie-Informations-System (RIS)
- Patientendaten benötigen oftmals den Kontext aus anderen Informationssystemen. Z. B.
  - Rechtfertigende Indikation zur Röntgenuntersuchung (§ 23 RöV) basiert auf Informationen des KIS
  - Werden Daten aus KIS gelöscht, ist ggf. Richtigkeit der rechtfertigenden Indikation nicht länger überprüfbar
- Bei Weitergabe an Externe: diese müssen über Löschung informiert werden (Art. 19 DS-GVO)
  - Weiß man zum Löschzeitpunkt noch, an welche externen Personen man die Daten weitergab?

Problemstellung: Heterogene Speicherdauer

Gesetzliche Aufbewahrungszeiträume unterschiedlich

– Gesetzliche Speicherdauern nicht einheitlich geregelt, z. B.

- Patientenakte: 10 Jahre nach Abschluss Behandlung, soweit keine anderen Vorschriften (§630 f Abs. 3 BGB)
- Berufsgenossenschaftliche Verletzungsverfahren: 15 Jahre (Ziff. 3.6.8 VAV i. V. m. § 33 SGB VII)
- Nosokomiale Infektionen: 10 Jahre (§ 23 Abs. 4 IfSG)
- Röntgenbehandlung: 30 Jahre (§ 28 Abs. 3 RöV)
- Röntgenbilder, Aufzeichnungen: 10 Jahre (§ 28 Abs. 3 RöV)
- Angaben zur rechtfertigenden Indikation: 10 Jahre (§ 85 Abs. 3 StrlSchV)
- Angaben zur Blut-Spenderdokumentation, Rückverfolgbarkeit: 30 Jahre (§11 Abs. 1 S. 2 TFG)
- Immunisierungsprotokolle: 20 Jahre (§8 Abs. 3 i. V. m. § 11 Abs. 1 TFG)
- ...

Mythos: Alles 30 Jahre aufbewahren…

Gesetzliche Aufbewahrungszeiträume unterschiedlich

- Heterogene Zeiten erschweren Löschung von Patientendaten, da diese oftmals nur im Kontext interpretierbar sind
- Häufig unterbreiteter Vorschlag: aus Haftungsgründen 30 Jahre aufbewahren
- Haftungsfristen
  - Regelmäßige Verjährungsfrist: 3 Jahre (§ 195 BGB)
    Beginn der Zeitrechnung: Person erlangte Kenntnis oder hätte Kenntnis ohne grobe Fahrlässigkeit erlangen müssen
  - Schadensersatzansprüche, die auf der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit beruhen, verjähren ohne Rücksicht auf ihre Entstehung und die Kenntnis oder grob fahrlässige Unkenntnis in 30 Jahren von der Begehung der Handlung, der Pflichtverletzung oder dem sonstigen, den Schaden auslösenden Ereignis an (§ 199 BGB)
  - Nach 30 Jahren: alles verjährt (§ 197 BGB)

Mythos: Alles 30 Jahre aufbewahren…

Also alles 30 Jahre aufbewahren?

- Jain. Grundsätzlich
  - Legitimer Verwendungszweck der Daten der Gesundheitsversorgung seitens des Leistungserbringers = Möglichkeit, sich gegen unrechtmäßige Schadensersatzansprüche wehren zu können
  - 30jährige Aufbewahrung erlaubt, wenn hinreichender Tatbestand auf einen Rechtsstreit besteht
  - Entfällt die Möglichkeit einer entsprechende Klage (z.B. durch Tod des Patienten, keine Erben vorhanden), müssen Daten nach Ablauf der Aufbewahrungsfrist und nach Eintreten des Ereignisses, welche eine Klage unmöglich macht, gelöscht werden
- Auslegung in Literatur sehr unterschiedlich
  - Löschung kann bleiben, wenn Erhebung gerichtlicher/außergerichtlicher Ansprüche nicht ausgeschlossen werden können
  - Überwiegende Ansicht: Erlaubte Aufbewahrungszeit abhängig, wie konkret zeichnet sich eine gerichtliche Auseinandersetzung ab?
- D.h. Löschung kann nur unterbleiben, wenn **Rechtsstreit** ansteht oder mit **hinreichender Wahrscheinlichkeit** zu **erwarten** ist

S. a. : Kühling J, Klar M. (2014) Löschpflichten vs. Datenaufbewahrung Vorschläge zur Auflösung eines Zielkonflikts bei möglichen Rechtsstreitigkeiten. ZD 10: 506-510

Mythos: Alles 30 Jahre aufbewahren…

Aufbewahrung aus Haftungsgründen = Risikoabwägung erforderlich

Gesetzliche Aufbewahrungsfrist abgelaufen und Daten sollen aus Haftungsgründen aufbewahrt werden

a) Konkreter Rechtsstreit steht an oder

b) Risikoabwägung erforderlich: Wie wahrscheinlich ist ein Rechtsstreit?

- Z. B. Untersuchung, wie oft bei bestimmten Eingriffen ein Rechtsstreit nach Ablauf der gesetzlichen Aufbewahrungsfrist erfolgte
- Nutzung der Daten aus den Rechtsstreitigkeiten z.B. der letzten 5 Jahre
- Ergebnis Risikoabwägung z.B.
  - Bypass-OP Kardiochirurgie: 5% Streitigkeiten nach Ablauf der 10jährigen gesetzlichen Aufbewahrungsfrist → Akten werden entsprechend der Frist, in welcher ein Rechtsstreit wahrscheinlich ist, aufbewahrt
  - Enukleation: 0% Rechtsstreit nach Ablauf der 10-Jahres-Frist → sofortiges Löschen

Mythos: Alles 30 Jahre aufbewahren…

Aufbewahrung aus Haftungsgründen = Risikoabwägung erforderlich

b) Risikoabwägung erforderlich: Wie wahrscheinlich ist ein Rechtsstreit?

- Risikogrenze selbst definieren
- Aber Höhe des Risiko, dass man tragen will, muss zum Haus passen
- Andere Risiken, die man eingeht, berücksichtigen. Beispiele
  - Risiko bzgl. IT-Sicherheitsvorfällen
    - Gut geschultes Personal für Firewall, Virenschutz usw. vorhanden?
    - Werden regelmäßig Penetrationstests durchgeführt.
    - Erfolgt ein jährliches externes Audit?
    - Existiert eine Zertifizierung?
  - Risiko bzgl. rechtlicher Rahmenbedingungen. Z.B. Motto „Lücke und nicht erwischt werden“ bzgl.
    - Mitarbeiterschulungen
    - formelle Anforderungen Arbeitsschutz/Datenschutz/Hygiene

Sicht der Hersteller: Löschen in med. Informationssystemen

Umgang mit „Löschen“

- Löschen: eindeutige gesetzliche Pflicht
  - Löschpflicht auf Verlangen des Betroffenen: §§ 14, 27 BDSG (1977)
  - Allgemeine Löschpflicht §§ 20, 35 BDSG (1990)
  - → Fazit: Jedes System, welches auf dem deutschen Markt seit 1990 angeboten wird, muss „seine“ Daten löschen können
- Entscheidung, ob Daten gelöscht werden dürfen oder nicht
  - Grundsätzlich von Anwender zu treffen
  - Rein automatisierte Löschung aus Gründen der Patientensicherheit abzulehnen
  - → Bedingt Regelung seitens datenverarbeitender Stelle: Wer entscheidet, welche Daten gelöscht werden dürfen?
- Konsistentes Löschen über IT-Systemgrenzen hinweg = Erfordernis, über Notwendigkeit der Datenlöschung zu kommunizieren
  - Beispiel: KIS sagt „Löschen“, PACs sagt „nicht Löschen, weitergehende gesetzliche Anforderungen“
  - Erweiterung Kommunikationsschnittstellen erforderlich

bvitg: Stellungnahme zum Löschen von Personenbezogenen Daten und Patientendaten in Krankenhausinformationssystemen (2015) http://www.bvitg.de/positionspapiere.html

Sicht der Hersteller: Löschen in med. Informationssystemen

Umgang mit „Löschen“

- Workflow Definition seitens Anwender erforderlich: Wann darf, wann muss gelöscht werden?
  - Berücksichtigung aller Umstände (gesetzliche Aufbewahrungszeiten, Haftungsregelungen, Zugriff auf Patientendaten bei erneuter Aufnahme, ...) erlaubt keine eindeutige automatisierte Zuordnung eines Löschdatums
  - Erfolgt fallbezogene oder dokumentenbasierte Löschung?
    - Letztlich existieren Regelungen für bestimmte Dokumententypen, z.B. Rezepte
    - Alle Patientendaten zusammen bilden die Patientenakte entsprechend § 630f BGB; Sinnhaftigkeit der Akte nur gegeben, wenn alle benötigten Informationen verfügbar dies spricht für ein fallbezogenes Löschen
- bvitg befand sich 2013 mit Aufsichtsbehörde (AK Medizin/Soziales) und DKG im Gespräch, konkrete Ergebnisse liegen nicht vor

Sicht der Hersteller: Löschen in med. Informationssystemen

„Erwartungskonformes“ Löschen = Papierkorb?

- EDV-Anwender
  - Löschen = „in den Papierkorb verschieben“
  - Löschen kann ungeschehen gemacht werden
- Was ist „erwartungskonformes“ Löschen für einen EDV-Anwender?
  - Darstellung auch dieses Workflows erforderlich
- Schulung erforderlich
  - Ansonsten ist ein Datenverlust und damit ggf. die Gefährdung von Patientenleben nur eine Frage der Zeit

Löschen unter der DS-GVO

Aktives Vorgehen, passives Abwarten?

- Bisher keine Sanktionen seitens Aufsichtsbehörden für nicht erfolgtes Löschen
- Sanktioniert wird „Verantwortlicher“
- Zweimögliche Vorgehensweisen
  a) Nichts tun und abwarten
     - Allerdings potentielles Bußgeld entsprechend Art. 83 Abs. 5 lit. b DS-GVO (=„hohes“ Bußgeld)
  b) Zusammenarbeit Verantwortlicher und IT-System-Hersteller bzgl. Löschen
     - Workflow muss erarbeitet werden
     - Löschung implementieren

Datenübertragbarkeit

Art. 20 DS-GVO: Recht auf Datenübertragbarkeit

Was gehört alles dazu?

- Recht, die sie betreffenden pbD, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten
- Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die Daten bereitgestellt wurden, zu übermitteln
- Recht gilt, sofern
  - die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und
  - die Verarbeitung mithilfe automatisierter Verfahren erfolgt

Art. 20 DS-GVO: Recht auf Datenübertragbarkeit

Begriffsbestimmungen

Bereitstellung

- Art. 4 Ziff. 2 DS-GVO: „[...] die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung [...]“
- Bereitstellung = Form der Verarbeitung
- EU-Richtlinie „über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte“:
  „'Bereitstellung' die Verschaffung des Zugangs zu oder die Zurverfügungstellung von digitalen Inhalten“
- Bereitstellung durch oder durch Unterstützung der betroffene Person

Art. 20 DS-GVO: Recht auf Datenübertragbarkeit

Begriffsbestimmungen

Strukturiertes, gängige und maschinenlesbares Format, ErwGr. 68 ergänzt „interoperables Format“

- Keine Legaldefinition für Begrifflichkeiten, jedoch in der IT-Welt definiert
- Strukturiert: Daten weisen eine gleichartige Struktur auf
- „Gängiges Format“: allgemein üblich, „normal“ ⟶ auf Norm basierend
- Maschinenlesbar: Objekte/Dokumente sind speziell darauf ausgelegt, für IT-Systeme lesbar zu sein; ggf. auch für Menschen lesbar
- Interoperabel: direkte Einlesemöglichkeit in das IT-System des empfangenden Verantwortlichen ist vorhanden

Art. 20 DS-GVO: Recht auf Datenübertragbarkeit

Beschränkung des Rechts

Art. 20 Abs. 3 DS-GVO

- Datenverarbeitung ist erforderlich
  - für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt
  - für die Wahrnehmung einer Aufgabe in Ausübung öffentlicher Gewalt
- ErwGr. 68: „Erfüllung einer rechtlichen Verpflichtung“
  - Beispiele im ErwGr: Archiv-, Forschungs- oder statistische Zwecke

Widerspruchsrecht

Recht zum Widerspruch

Jeder darf einer Verarbeitung widersprechen

- Jederzeit gegen die Verarbeitung personenbezogener Daten widersprechen, wenn
  - Datenverarbeitung aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt
- Verarbeitung zu Direktwerbung
  - Widerspruchsrecht unabhängig von allen Bedingungen
- Verarbeitung bzgl. wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken
  - Vollständiges Widerspruchsrecht
  - Aber: Verarbeitung erfolgt zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe ⟶ Kein Widerspruchsrecht

Recht zum Widerspruch

Jeder darf einer Verarbeitung widersprechen

Folgen Widerspruch

- Daten werden nicht mehr für diese Zwecke verarbeitet
- Cave:
  - Sperrung oder Löschung sind nicht explizit gefordert, aber jegliche Verarbeitung (inkl. Speicherung) zu diesem Zweck ist verboten
  - D. h.: kein anderer Verarbeitungszweck oder keine Rechtsgrundlage für Speicherung ⟶ Widerspruch bedingt Löschung der Daten

Automatisierte Einzelfallentscheidung

Automatisierte Einzelfallentscheidung

Scoring, Profiling & Co.

- Entscheidung ausschließlich auf einer automatisierten Verarbeitung beruhend:
  - Verboten, wenn diese Entscheidung rechtliche Wirkung gegenüber einer Person entfaltet oder die Person „in ähnlicher Weise erheblich beeinträchtigt“
- Ausnahmen
  - Abschluss oder die Erfüllung eines Vertrags zwischen betroffener Person und Verantwortlichen
  - Gesetz, welchem der Verantwortliche unterliegt, schreibt dies vor
    - Cave: Gesetz muss entsprechende Schutzrechte aufweisen
  - Ausdrückliche Einwilligung liegt vor

→ Cave: **Ausnahmen** (abgesehen von Einwilligung sowie gesetzlicher Forderung) **gelten nicht** für besondere Kategorien von Daten

Automatisierte Einzelfallentscheidung

Scoring, Profiling & Co.

Wenn Ausnahme genutzt wird, muss Verantwortlicher

- Maßnahmen zur Wahrung der Betroffenenrechte ergreifen
- Die berechtigten Interessen der betroffenen Person berücksichtigen
- Möglichkeit für betroffene Person schaffen, Ansprechpartner bei Verantwortlichen zu erreichen, der
  - Welcher die betroffene Person den eigenen Standpunkt darstellen kann
  - Welchem die betroffene Person gegenüber die Entscheidung anfechten kann
  - bei Entscheidungsfindung eingreifen kann

BDSG n.F.

Scoring, Profiling & Co.

- Das Recht bzgl. automatisierter Einzelfallentscheidung gilt nicht,
- wenn Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht und
  - dem Begehren der betroffenen Person stattgegeben wurde oder
  - die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht und im Falle einer nicht umfänglichen Stattgebens des Antrags angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person traf

    Dazu gehörend
    - Recht auf Erwirkung des Eingreifens einer Person beim Verantwortlichen
    - Darlegung des eigenen Standpunkts
    - Anfechtung der Entscheidung