

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Datenschutzfolgenabschätzung

DATEN
SCHUTZ!

1

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.



- Auszug Vita Michael Letter
- Studium Betriebswirtschaft GH Duisburg
- Gründung der 5medical management GmbH 1996
- Seit 12 Jahren im Bereich Datenschutz spezialisiert
- Mitautor der GDD Praxishilfen und der GMDS – Ratgeber
- Referent zum Thema DSFA

Kontakt info@letter-consulting.de
www.5medical-management.de
Tel: 02131 1331166

2

gmds Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.

Agenda

- Kurze Beleuchtung des Art. 35 DS-GVO
- Blacklists der Aufsichtsbehörden, wann ist eine DSFA durchzuführen?
- Forschung und DSFA
 - Forschungsprivileg und Dokumentation
 - Auffassung LDI Rheinland-Pfalz
 - Checkliste Forschung
- Grundsätze bei einer DSFA
 - Exkurs Drittlandtransfer
- DSFA welche Tools
 - Praktisches Arbeiten mit der PIA und dem Tool der GMDS
- Fragerunde

3

gmds Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.

Hinweis

Die Präsentation wird zur Verfügung gestellt

Vortrag bis ca. 15.30 im Anschluss Fragen und Diskussion

Gern zwischendurch eine kurze Pause

Fragen, gern auch zwischendurch an die Moderatorin im Chat

4



Art. 35 DSGVO

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

Für die Untersuchung **mehrerer ähnlicher** Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

5



Art. 35 DSGVO

Für die Untersuchung **mehrerer ähnlicher** Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.



Für Forschungszwecke oder Zwecke in der Klinik spannend, wenn es ähnlich oder gleichgelagerte Forschungsvorhaben oder Verarbeitungen gibt.

Achtung Begründung dokumentieren.

6

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Art 35 DSGVO

- Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 erforderlich:
- a) systematische und umfassende Bewer- tung sich auf automatisierte Verarbeitung ei- ner Person als Grundlage für Entscheidungen dient, die ähnlich erheblicher Weise be- ... entfalten oder diese in
- b) **umfangreiche** Verarbeitung besonderer Kategorien von personenbezogenen Daten **gemäß Artikel 9 Absatz 1** oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
- c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

Z. B. Forschung ja
Kliniken ja
MVZ meist ja
Praxen kommt drauf an

7

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.



DSK
DATENSCHUTZKONFERENZ

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist			
Nr.	Mögliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfälle	Beispiele
1	Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: <ul style="list-style-type: none"> • Daten zu schutzbedürftigen Betroffenen • Systematische Überwachung • Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen • Bewerten oder Einstufen (Scoring) • Abgleichen oder Zusammenführen 	Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke.	Ein Unternehmen setzt flächendeckend Fingerabdrucksensoren zur Zutrittskontrolle für bestimmte Bereiche ein. Eine Schulkantine bietet den Schülern das „Bistrotten per Fingerabdruck“ an.

Blacklist der Aufsichtsbehörden

<https://www.datenschutzkonferenz-online.de/kurzpaepiere.html>

8



Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.

Die Landesbeauftragte für
Datenschutz und
Informationsfreiheit



Freie
Hansestadt
Bremen

**Liste von Verarbeitungsvorgängen nach Artikel 35
Absatz 4 Datenschutzgrundverordnung,**
für die gemäß Artikel 35 Absatz 1 Datenschutzgrundverordnung eine Datenschutz-
Folgenabschätzung bei Verantwortlichen im öffentlichen Bereich erforderlich ist.

Stand: 25.03.2021

<https://www.datenschutz.bremen.de/sixcms/media.php/13/Liste%20von%20Verarbeitungsvorg%E4ngen%20nach%20Artikel%2035.pdf>

9



Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.

Im medizinischen Umfeld ist eine DSFA
durchzuführen:

Umfangreiche Verarbeitung von Daten gemäß Artikel 9 Absatz 1

- Krankenhausinformationssystem
- Ggf. MVZ (Patientendaten werden zentral verwaltet)



10

gmnds Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.

Im medizinischen Umfeld ist eine DSFA durchzuführen:

Anonymisierung von besonderen personenbezogenen Daten z. B.

- Übermittlung an nicht-gesetzlich geregelte Krankheitsregister
- Forschung
- auch eventuelle Nutzung zur Qualitätssicherung



11

gmnds Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.

Im medizinischen Umfeld ist eine DSFA durchzuführen:

- Verarbeitung von Art. 9 Daten, sofern eine nicht einmalige Datenerhebung mittels Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden (z.B. Telemedizin-Anwendungen)



12

Im medizinischen Umfeld ist eine DSFA durchzuführen:

- Verarbeitung von Art. 9 Daten durch zentrale Internetdienste z.B.
 - Verarbeitung von Gesundheitsdaten in der Cloud
 - institutionsübergreifende Patientenakten (z. B. Klinik + Strahlentherapie)
 - Offen "ePA"

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.



13

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Exkurs
Forschung und DSFA

14

gmds Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.

Forschungsprivileg
DSGVO, BDSG, ggf.
Landesgesetzte

- Zulässigkeit = DSGVO (allerdings ist dort Forschung nicht definiert), Rechtsgrundlagen Art 6 in Verbindung mit Art 9 Gesundheitsdaten
- Transparenzpflichten Art 5 (Nachweise, Dokumentation)
- BDSG-neu §27 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken (Einschränkung der Betroffenenrechte (Art. 15,16,18 und 21)
- LKG Rheinland-Pfalz § 37 Datenschutz bei Forschungsvorhaben (Einwilligungen)

15

gmds Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.

Forschungsprivileg
DSGVO, BDSG, ggf.
Landesgesetzte

- Transparenzpflichten Art 5.2 (Nachweise, Dokumentation, Rechenschaftspflicht)
- Wie beschreibt u. a. Art. 30 Verarbeitungsübersicht (VVT)
- Daraus folgt = Forschungsprojekte sind ins VVT aufzunehmen
- ggf. können gleichlautende Studien oder gemeinsame Studien zusammengefasst werden. (Begründung liefern)
- Die Rechenschaftspflicht bedingt eine Dokumentation und Art. 35 DSGVO die Durchführung einer Datenschutzfolgenabschätzung (Blacklist der DSK)

16

gmds Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.

- [Checkliste Forschung DSGVO 2.8.pdf](#)

Rae Marc Rüdlin, Hamburg

Diese Vorlage können Sie gern bei mir per Mail anfordern.

Checkliste
Datenschutzbelange bei Forschungsprojekten

Bezeichnung des Forschungsprojekts:			
Kurzbeschreibung:			
Voraussichtlicher Beginn des Forschungsprojekts:		Voraussichtliches Ende des Forschungsprojekts:	

	Rechtsgrundlage	Ja	Nein	Anmerkungen
1. Grundrechtsprüfung				
Benötigt das Forschungsvorhaben Patientendaten?	EG 159 zur DSGVO	<input type="checkbox"/>	<input type="checkbox"/>	
Keine unangemessene Beeinträchtigung des Patienten durch Bedarf an Patientendaten?	Art. 2 Abs. 1 GG	<input type="checkbox"/>	<input type="checkbox"/>	

17

gmds Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.



Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz



Prof. Dr. Dieter Kugelmann

Auffassung

- Bei der Forschung im medizinischen Bereich ist eine Datenschutzfolgenabschätzung gemäß Art. 35 DS-GVO unerlässlich.

18



Arbeits- und Praxishilfen

- Arbeitshilfe der GMDS zur Pseudonymisierung/Anonymisierung vom 29. Juni 2018
https://gesundheitsdatenschutz.org/html/pseudonymisierung_anonymisierung.php
- Die Praxishilfe „Datenschutz bei Klinischen Studien“
(https://gesundheitsdatenschutz.org/html/klin_studien.php, Stand 10. Dezember 2019) Für Forscher interessant, auch wenn Anonymisierung nur sehr kurz erwähnt wird. Aber datenschutzrechtliche Anforderungen für medizinische Forscher wurden gut dargestellt.
- Die Praxishilfe „Klinische Register und Datenschutz“
(https://gesundheitsdatenschutz.org/html/klin_register.php, Stand 13. Dezember 2019) betrifft medizinische Forschung eigentlich nur indirekt, aber Kapitel 12.5 betrifft die Anonymisierung. Auch wenn es kurz ist, könnte Abschnitt 12.5.1 von Interesse sein.

In der Forschung kann man sehr viel falsch machen. Bei der Frage zur Anonymisierung ist es oft richtig ihre zuständige Aufsichtsbehörde anzusprechen.

19



Exkurs Drittlandtransfer

- GDD / Bitkom etc. empfehlen Risikobetrachtung
- EuGH Schrems II „Betroffenenrechte gewährleisten im Drittland“
- Rechte im Drittland betrachten (Art. 2 innerhalb EU, ist die Überwachung möglich, sobald außerhalb der EU z. B. USA 2018 Cloud Act „Clarifying Lawful Overseas Use of Data Act“ nicht mehr.

20

Exkurs Drittlandtransfer



Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.

- Risikobetrachtung mittels DSFA z. B. betrachten wie wahrscheinlich ist ein Zugriff nach dem Cloud Act – „Clarifying Lawful Overseas Use of Data Act“ auf med. Daten von Michael Letter in einem Kreiskrankenhaus – höchst unwahrscheinlich
- Bei medizinischen Daten von einem Minister in der Charité in Berlin, kann sich ein anderes Ergebnis herausstellen.
- **Hinweis** - keine Aufsicht hat sich bisher dazu geäußert, ob eine DSFA sinnvoll ist.
- Sie haben aber bestmöglich das Risiko betrachtet und ihre Entscheidung abgewogen
- Hinweis: Mailchimp BayLDA

21

Grundsätze der Dateschutzfolgenabschätzung



Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.



22

Grundsätze bei einer DSFA

- G l#S VID# xv#q#ghu#Jhjh#ehulw#ru#ghu#
Hl ixkxqj #ghv#hudeh lwqjvyhuidkuhv#
gxufkjhixku#kqg#gdqdfk#q#hjhq îÖljhq#
Dewlqgghq# lghukro# hughq1
- Ghu# z hfn#kqg#gh#Uhfkwjuxqgajh#vlg#x#
ehvfkulehq#deh#rön#nz hlv# Âjdfkw#nrqnuw#
yrujhdqjhg# hughq1
- G ddx i#r ojw#lqh#Ehz huwqj #ghv#Jlvhrv#xu#gh#
Uhfkw#kqg#uhlkhlhg#ghu#hwr iihqg#Shwrqhg#
Z hwhuk l#v#h#Sux ixqj #ghu#huk îoqlp îÖljnhlw#
eh}xjdfk#ghv#huk îoqlvvhv#ghu# z hfn#x#ghq#
gdwhqvfkxw)uhfkwdfkhq#Jlvhhq#huirghudfk1



Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.



23

Grundsätze bei einer DSFA

- Dx i#ghu#Uxqgajh#ghu#Jlvrehz huwqj#p xvvhq#gh#
Vlfkhukhlwp dÖqdkp hq#ghilqlnuw# hughq1
- Dönv#Exv#ghu#Vfkw#ghu#Ehwr iihqg
- J j i#lqghu#Dnwuxu#hqvfkdohg#
-G dwhqvfkxw)dx ivfkw#Ehwr iihqh# }z #hwhwhu,
- Vrz hlv# Âjdfk#shwrqhgqeh}rjhqh#G dwhq#
dqrq |p lvhuhq



Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.



24

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

DSFA
Prüfschemen

Eigene Methoden

Die Landesbeauftragte für den Datenschutz
Niedersachsen

25

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

DSFA
durchführen
mit..

Nur einige Möglichkeiten

- Das Standard-Datenschutzmodell
- ISO/IEC 29134 "Guidelines for privacy impact assessment"
(Stand 2017-06 beuth.de LDA Bayern Herr Sax)
- Bitcom - Risk Assessment & Datenschutz-Folgenabschätzung
- PIA der französischen Aufsichtsbehörde CNIL
- Werkzeug der GMDS und bvitg
- Parallele Anwendung diverser Werkzeuge

26



Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.

Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V. 

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und
Epidemiologie e. V. 
Arbeitskreis „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Deutsche Krankenhausgesellschaft e. V. 

Autoren

Ina Haag	Deutsche Krankenhausgesellschaft e.V.
Andreas Häuser	Deutsche Krankenhausgesellschaft e.V.
Christoph Iselt	Cerner Deutschland GmbH
Lukas Mempel	Sana Kliniken AG
Christoph Nahrstedt	Nuance Communications
Jen Neuhäus	Deutsche Krankenhausgesellschaft e.V.
Bernd Schülze	Deutsche Telekom Healthcare and Security GmbH
Gerold Spyrig	Ratapack und Partner mbB Rechtsanwälte
Stefan Wunschel	Sana Kliniken AG

Stand: 10.04.2018

<https://gesundheitsdatenschutz.org/html/dsfa-beispiel.php>

27



Deutsche Gesellschaft für
Medizinische Informatik,
Biometrie und
Epidemiologie e.V.

Tipps

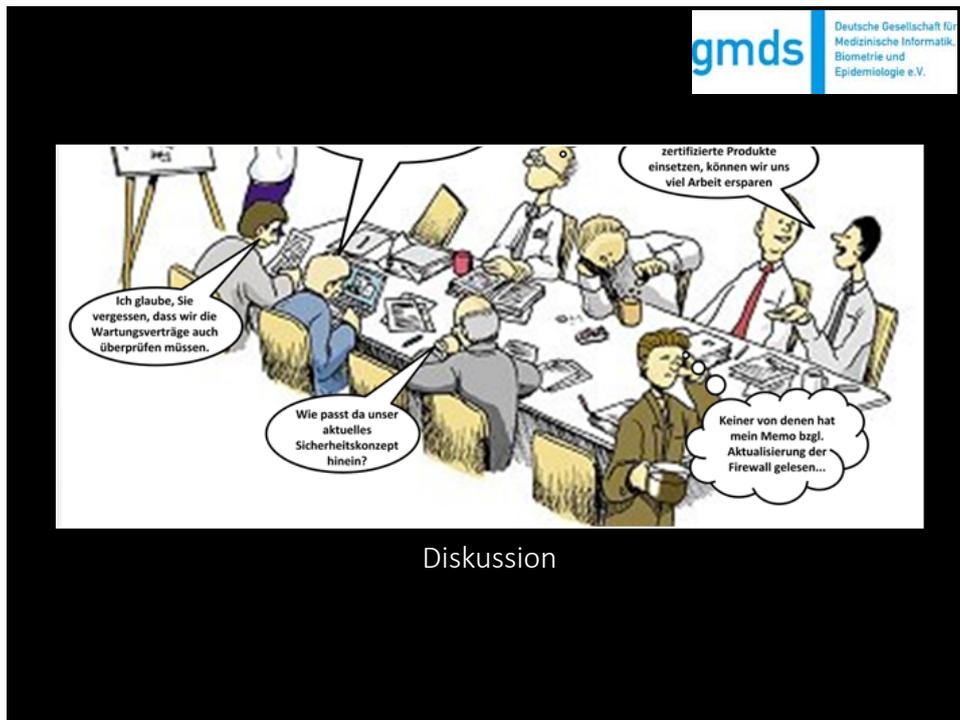
Die Beteiligten zu aktiven Teilnehmern machen

Vorstände/Klinikleitungen/etc. mitnehmen

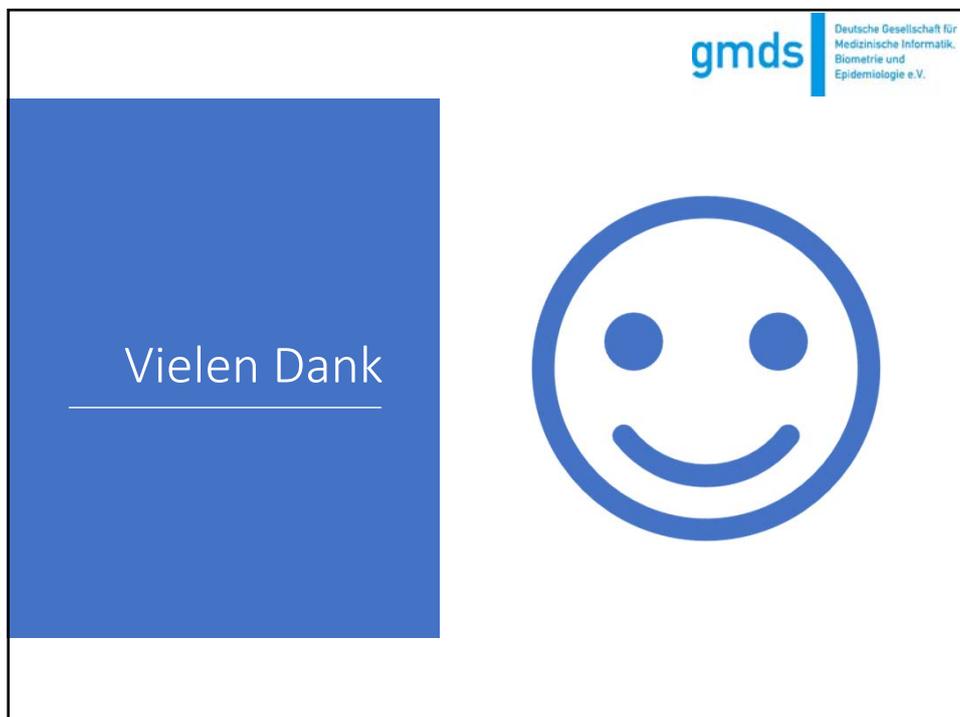
Mögliche Argumente:

- „Planspiel, es geht auch um die Assets“
- „Es ist eine Vorsorge, wie eine Art Versicherung“

28



31



32