CNIL.

To protect personal data, support innovation, preserve individual liberties

DATA PROTECTION | TOPICS | THE CNIL |

> Privacy Impact assessment (pia)

Privacy Impact assessment (pia)

Where a processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out a privacy impact assessment.

DPIA guidelines

PIA Software

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

Agenda

- Kurze Einführung Art. 35
- Blacklists der Aufsichtsbehörden
- Risikobewertung
- Anhand des Tools PIA eine DSFA anlegen
- Fragerunde

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.

Art 35 DSGVO

- Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

- a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

- 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;

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

Blacklist der Aufsichtsbehörden

DSK DATENSCHUTZKONFERENZ

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
1	Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: • 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 „Bezahlen per Fingerabdruck“ an.

Blacklist der Aufsichtsbehörden

3	Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, auch wenn es sich nicht um Daten gemäß Art. 9 Abs. 1 und 10 DS-GVO handelt	Betrieb eines Insolvenzverzeichnisses Träger von großen sozialen Einrichtungen Große Anwaltssozietät	Ein Unternehmen bietet ein umfassendes Verzeichnis über Privatinsolvenzen an. Große Rechtsanwaltskanzlei, die im Schwerpunkt familienrechtliche Mandate betreut.
4	Umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen	Fahrzeugdatenverarbeitung – Car Sharing / Mobilitätsdienste	Ein Unternehmen bietet einen Car-Sharing-Dienst oder andere Mobilitätsdienstleistungen an und verarbeitet

Im medizinischen Umfeld ggf. auch zu beachten:

- Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Weiterverarbeitung der so zusammengeführten Daten (z.B. Big Data, Data-Warehouse)

- Erhebung personenbezogener Daten über Schnittstellen persönlicher elektronischer Geräte, die nicht gegen ein unbefugtes Auslesen geschützt sind (z.B. Einsatz von Tracking mittels RFID-Chips)

- Anonymisierung von besonderen personenbezogenen Art. 9 Daten (z.B. Übermittlung an nicht-gesetzlich geregelte Krankheitsregister, Forschung, evtl. Nutzung zur Qualitätssicherung)

- 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)

- Verarbeitung von Art. 9 Daten durch zentrale Internetdienste (z.B. Verarbeitung von Gesundheitsdaten in der Cloud, institutionsübergreifende Pat.-Akten)

Risiko-Checkliste

- Risikofaktoren nach Datenarten
- Risiko steckt in der Verarbeitung
- Nach Gefährdungspotenzial
- Risiko nach sonstigen Kriterien

Ermittlung von Risiken der Verarbeitungstätigkeiten

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

Quelle: 3. Schema zur Ermittlung von Risiken der Verarbeitungstätigkeiten, Witt in Formularhandbuch Datenschutzrecht, Seite 211 ff., Koreng, Lachenmann, 2. Auflage 2018, C. H. Beck

Nr.	***Datenart***	***ja***	***nein***
1	Daten über die rassische oder ethnische Herkunft		
2	Daten über politische Meinungen		
3	Daten über religiöse oder weltanschauliche Überzeugungen		
4	Daten über die Zugehörigkeit zu einer Gewerkschaft		
5	Genetische Daten		
6	Biometrische Daten zur eindeutigen Identifizierung		
7	Gesundheitsdaten		
8	Daten über das Sexualleben oder der sexuellen Orientierung		
9	Daten über strafrechtliche Verurteilungen oder Straftaten		
10	Daten zur Bewertung der Arbeitsleistung		
11	Daten zur Bewertung der wirtschaftlichen Lage		
12	Daten zur Bewertung der Gesundheit		
13	Daten zur Bewertung persönlicher Vorlieben oder Interessen		
14	Daten zur Bewertung der Zuverlässigkeit		
15	Daten zur Bewertung des Verhaltens		
16	Daten zur Bewertung des Aufenthaltsortes oder von Ortswechsel		
17	Daten von Kindern		

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

Nr.	*Faktor* Verarbeitung	*ja*	*nein*
1	Bei der Verarbeitung soll eine neue, bisher noch nicht in einer Datenschutz-Folgenabschätzung untersuchte Informations- und Kommunikationstechnik eingesetzt werden.		
2	Bei der Verarbeitung soll eine hochkomplexe und stark miteinander vernetzte Informations- und Kommunikationstechnik eingesetzt werden.		
3	Bei der Verarbeitung soll eine große Menge personenbezogener Daten verarbeitet werden.		
4	Von der Verarbeitung ist eine große Anzahl von Personen betroffen.		
5	Die Verarbeitung dient der systematischen und umfangreichen großflächigen Überwachung im öffentlichen Raum.		
6	Die Verarbeitung soll teilweise oder vollständig (z. B. hinsichtlich Speicherung, Datensicherung oder Fernwartung) in einem Drittland durchgeführt werden, welches gemäß der Rechtsauffassung der EU-Kommission über kein angemessenes Datenschutzniveau verfügt.		
7	Die Verarbeitung ermöglicht eine umfassende und mit dem ursprünglichen Zweck der Datenerhebung nicht unmittelbar vereinbare Verknüpfung und Auswertung der gespeicherten Daten unter Berücksichtigung von Art. 6 Abs. 4 DS-GVO.		
8	Für die Verarbeitung sollen zahlreiche Auftragsverarbeiter eingesetzt werden, die über einen Fernwartungszugang verfügen.		
9	Die Verarbeitung ermöglicht den Betroffenen keinerlei Form einer unmittelbaren Kontrolle ihrer Daten (z. B. vom Betroffenen aufrufbare Anzeige der über ihn gespeicherten Daten) oder erschwert den Betroffenen die Ausübung ihrer Rechte entgegen der Vorgabe aus Art. 12 Abs. 2 DS-GVO.		
10	Die Verarbeitung soll zu einer automatisierten Entscheidungsfindung führen, die gegenüber dem Betroffenen eine rechtliche Wirkung entfaltet oder den Betroffenen in ähnlicher Weise erheblich beeinträchtigt, ohne dass der Betroffene seinen Standpunkt zur Anfechtung der Entscheidung vortragen kann.		
11	Die Verarbeitung kann die Betroffenen an der Nutzung einer Dienstleistung bzw. an der Durchführung eines Vertrags hindern.		
12	Die Verarbeitung befindet sich auf der von Aufsichtsbehörden veröffentlichten Liste nach Art. 35 Abs. 4 DS-GVO über Verarbeitungsvorgänge, zu denen eine Datenschutz-Folgenabschätzung durchzuführen ist.		

Nr.	*Gefährdungspotenzial*	*ja*	*nein*
1	Die unbefugte Verwendung der gespeicherten Daten ermöglicht eine Diskriminierung des Betroffenen.		
2	Die gespeicherten Daten können von einem Unbefugten für Identitätsdiebstahl oder Identitätsbetrug verwendet werden.		
3	Eine unbefugte Verwendung der gespeicherten Daten kann für den Betroffenen zu einem finanziellen Verlust führen.		
4	Eine unbefugte Verwendung der gespeicherten Daten kann für den Betroffenen zu einer Rufschädigung führen.		
5	Eine unbefugte Einsichtnahme in die gespeicherten Daten verletzt ein bestehendes Berufsgeheimnis, dem die personenbezogenen Daten unterliegen.		
6	Die Pseudonymisierung gespeicherter Daten kann von einem Unbefugten nach Zugriff auf die gespeicherten Daten aufgehoben werden.		
7	Eine unbefugte Verwendung der gespeicherten Daten kann für den Betroffenen zu einem erheblichen wirtschaftlichen Nachteil führen.		

Nr.	*Gefährdungspotenzial*	*ja*	*nein*
8	Eine unbefugte Verwendung der gespeicherten Daten kann für den Betroffenen zu einem erheblichen gesellschaftlichen Nachteil führen.		

Nr.	*Kriterium*	*ja*	*nein*
1	Ein Angreifer oder Störer benötigt für einen unbefugten Zugriff auf die gespeicherten oder übertragenen Daten nur alltägliche und weit verbreitete Informations- und Kommunikationstechnik und für seinen Angriff keine besonderen Spezialkenntnisse.		
2	Die gespeicherten Daten sind im verwendeten Informations- bzw. Kommunikationssystem komfortabel und bereits im Zuge vom Nutzer selbst erstellbarer Reports miteinander kombinierbar.		
3	Auf die gespeicherten bzw. übertragenen personenbezogenen Daten besteht für zahlreiche Nutzer ein umfassender Zugriff, um diese Daten wenigstens lesen zu können.		
4	Bei der Entwicklung der Software wurde weder der Grundsatz „Datenschutz durch Technikgestaltung“ noch der der Grundsatz „datenschutzfreundliche Voreinstellung“ berücksichtigt.		
5	In der Vergangenheit wurden bereits Verletzungen des Datenschutzes festgestellt (die Gründe, die dazu geführt haben, sind unerheblich).		
6	Beim Verantwortlichen bzw. Auftragsverarbeiter wird weder ein Datenschutzbeauftragter (bzw. Data Protection Officer) noch ein IT-Sicherheitsbeauftragter (bzw. Informationssicherheitsbeauftragter oder Chief Information Security Officer) eingesetzt.		
7	Der Schutz der personenbezogenen Daten basiert überwiegend darauf, dass die mit der Datenverarbeitung befassten Personen lediglich organisatorische Vorgaben einhalten müssen.		

Quelle: 3. Schema zur Ermittlung von Risiken der Verarbeitungstätigkeiten, Witt in Formularhandbuch Datenschutzrecht, Seite 211 ff., Koreng, Lachenmann, 2. Auflage 2018, C. H. Beck

DSFA durchführen mit..

Das Standard-Datenschutzmodell liegt zunächst in einer Erprobungsfassung vor. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Heinz Müller, bittet alle für die Verarbeitung personenbezogener Daten verantwortlichen Stellen, das SDM zu erproben und über die Erfahrungen bei der Anwendung des SDM zu berichten. Auf diese Weise soll die Praxistauglichkeit erprobt und die ständige Weiterentwicklung unterstützt werden.

ISO/IEC 29134 "Guidelines for privacy impact assessment" (Stand 2017-06) (beuth.de) (LDA Bayern Herr Sax)

Eigene Methoden

PIA der französischen Aufsichtsbehörde CNIL

Weiterführende Quellen

DATENSCHUTZGRUPPE NACH ARTIKEL 29

17/DE

WP 248 Rev. 01

Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“

angenommen am 4. April 2017

zuletzt überarbeitet und angenommen am 4. Oktober 2017

gmds 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.
Andrea Hauser	Deutsche Krankenhausgesellschaft e.V.
Christoph Isele	Cerner Deutschland GmbH
Lukas Mempel	Sana Kliniken AG
Christoph Nahrstedt	Nuance Communications
Jan Neuhaus	Deutsche Krankenhausgesellschaft e.V.
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Gerald Spyra	Ratajczak und Partner mbB Rechtsanwälte
Stefan Wunschel	Sana Kliniken AG

Stand: 10.04 2018


LIVE

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

Diskussion