



Das Verarbeitungsverzeichnis nach Artikel 30, DSGVO...

... und was hat das Verarbeitungsverzeichnis nach Art.
30, DSGVO mit klinischen Studien zu tun...?

- **CTR-Verordnung**
 - (536/2014: Clinical-Trials-Regulation) in Kraft seit 2014, gilt ab Mitte 2019
- **MDR-Verordnung**
 - (2017/745): Medical Device Regulation) in Kraft seit 2017, gilt ab Mai 2020
- **IVDR-Verordnung**
 - (2017/746): In-Vitro-Diagnostic-Regulation) in Kraft seit 2017, gilt ab Mai 2022.

Das Verarbeitungsverzeichnis nach Artikel 30, DSGVO

	 Christian-Albrechts-Universität zu Kiel Medizinische Fakultät	Verzeichnis von Verarbeitungstätigkeiten Artikel 30 Abs. 1, DSGVO	Seite 1 von 8
			Version: 001/11.2018
Campus Kiel			



I. Angaben zum Verantwortlichen

Kommentar: Bei medizinischer Forschung/Krankenversorgung: Vorstandsvorsitzender UKSH/Geschäftsführung der Tochtergesellschaft oder bei Forschungen Präsidium der CAU

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

- Universitätsklinikum Schleswig-Holstein
Campus Kiel
Vorstand
Arnold-Heller-Straße 3
24105 Kiel
www.uksh.de
Telefon (Zentrale): 0431 500-0

oder entsprechend die Anschrift der UKSH Tochtergesellschaften:

- Name:
Anschrift:
Homepage:
Telefon:

oder

- Christian-Albrechts-Universität zu Kiel
Präsidium
Christina-Albrechts-Platz 4
24118 Kiel




Warum ein Verarbeitungsverzeichnis?

- Ergibt sich aus den Grundsätzen der DSGVO (Artikel 5, Absatz 2, DSGVO): „Der Verantwortliche ist für die Einhaltung der Grundsätze... verantwortlich und muss dessen Einhaltung nachweisen können.
- Grundsätze für die Verarbeitung von personenbezogenen Daten sind u.a.: Zweckbindung, Datenminimierung, rechtmäßig erhalten,... (Artikel 5, Absatz 1, DSGVO).

Grundsätzliches zum Verarbeitungsverzeichnis

- Klärung, um welche Art/Form von Verarbeitungstätigkeit es sich handelt:
 - Bin ich allein verantwortlich?
 - Bin ich gemeinsam verantwortlich?
 - Verarbeite ich im Auftrag?
- Grundgerüst für das Verzeichnis
 - Pflichtangaben
 - Zusätzliche Dokumentation durch Angaben zu technischen und organisatorischen Maßnahmen (TOM's).

		Verzeichnis von Verarbeitungstätigkeiten Artikel 30 Abs. 1, DSGVO	Seite 1 von 8 Version: 001/11.2018
Campus Kiel			

I. Angaben zum Verantwortlichen
Kommentar: Bei medizinischer Forschung/Krankenversorgung: Vorstandsvorsitzender UKSH/Geschäftsführung der Tochtergesellschaft oder bei Forschungen: Präsidium der CAU
Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.
<input type="checkbox"/> Universitätsklinikum Schleswig-Holstein Campus Kiel Vorstand Arnold-Heller-Straße 3 24105 Kiel www.uksh.de Telefon (Zentrale): 0431 500-0
oder entsprechend die Anschrift der UKSH Tochtergesellschaften:
<input type="checkbox"/> Name: Anschrift: Homepage: Telefon:
oder
<input type="checkbox"/> Christian-Albrechts-Universität zu Kiel

		Verzeichnis von Verarbeitungstätigkeiten Artikel 30 Abs. 1, DSGVO	Seite 6 von 10 Version: 001/11.2018
Campus Kiel			

Struktur für die Dokumentation des ordnungsgemäßen Einsatzes von Informationstechnik (technische und organisatorische Maßnahmen (TOM), gemäß Art.32, Absatz 1, DSGVO)

1. Verfahrensdokumentation
1.1. Einsatz der von Informationstechnik
1.1.1. Darstellung des Verfahrenszwecks sowie die Maßnahmen zur Datenvermeidung und Datensparsamkeit (Datenminimierung)
Kommentar: Detaillierte Beschreibung, welche Verarbeitungszwecke das Verfahren realisiert und welche Daten dabei genutzt werden (Datenfeldbeschreibung):
Beispiele: <ul style="list-style-type: none">• Anordnung von Tagesmedikation• Plausibilitätskontrolle Verordnung• Vidierung Arzt, Apotheker• Kumulativstatistik Medikationskosten Station• Benachrichtigung von im Falle von• Anforderung von Zytostatika• Dokumentation Pflege IV-System• Anforderung Labor• Anforderung CT• ...

Wichtige Aspekte im Verarbeitungsverzeichnis

- Klärung von.....

- Wer ist der/die zuständige, behördliche Datenschutzbeauftragte/r?
- Welche Landesbehörde ist zuständig?
- Wenn gemeinsam verantwortlich - wie sieht es mit dem europäischen Vertreter aus?
- Wie wird verarbeitet?

- Klärung in der Dokumentation....

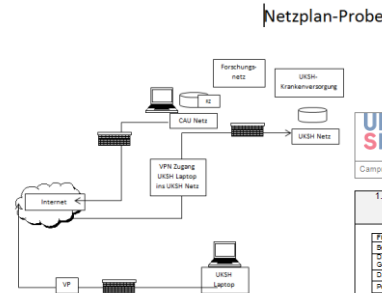
- In 1.1.2.: Benennung der Netze/Server/...
- In 1.1.4.: graphischer Netzplan
- In 1.1.5.: Berechtigungsvergabe

1.1.2. Darstellung der für das Verfahren verwendeten informationstechnischen Geräte einschließlich des Standorts

Kommentar: konkrete Benennung der Server, Kommunikationsserver, Clients, DB-Server, Sicherung, Gateways..... (→ alles an HW inkl. Inventarisierung). Wenn innerhalb des gesicherten Netzes des UKSH verarbeitet wird, Hinweis auf das IT-Sicherheitskonzept der ITSG oder andere RZ. Standorte: an Standorte außerhalb der ITSG/RZ denken

- ITSG Sicherheitskonzept
- Andere und zwar:

Schnittstellenbeschreibungen (physisch) → siehe 1.1.4



UKSH	CAU	Verzeichnis von Verarbeitungstätigkeiten Artikel 30 Abs. 1, DSGVO	Seite 8 von 10 Version: 00/11/2018
Campus Kiel			

1.1.5. Darstellung der technischen und organisatorischen Vorgaben für die Datenverarbeitung einschließlich der Darstellung, welche Personen für welche Aspekte der Datenverarbeitung verantwortlich und berechtigt sind

Für das Projekt verwendete Daten	Rolle 1	Rolle 2	Rolle 3	Rolle 4	Rolle 5	Rolle 6	Rolle 7
Beispiele	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
rolle: Artikel 4, DSGVO/ Teilnehmer (Name, Geburtsdatum, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Daten: Artikel 3, DSGVO/ Medizinische Daten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Personalisten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ärztliche/EGG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Personenidentifizierung/Anonymisierung	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zugriff pseudonymisierte Daten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zugriff anonymisierte Daten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zugriff „raw“	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Übermittlung der Daten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Empfang der Daten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- Beispiele
- Rolle 1: Studienleitung/Leitung Forschungsvorhaben
 - Rolle 2: Professor/Wissenschaftler
 - Rolle 3: Monitore/interne und externe Partner
 - Rolle 4: Studynurse
 - Rolle 5: Promovenden
 - Rolle 6: weitere StudienmitarbeiterInnen
 - Rolle 7: Pseudonymisierung-/Anonymisierungstelle
- Weitere Differenzierung nach Organisationseinheiten/Stellen (bitte eintragen)

Weitere, wichtige Gesichtspunkte....

- **Datenschutzfolgeabschätzung nach Artikel 35, DSGVO (DSFA)**
 - Wenn ein großes Risiko für die Rechte Betroffenen besteht
 - Immer wenn Daten nach Artikel 9, DSGVO (z.B. Gesundheitsdaten) verarbeitet werden
 - Formen/Arten der Verarbeitung, die in der „DSFS Liste“ der Datenschutzkonferenz (DSK) aufgeführt ist.



Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Mögliche 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:	Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke.	Ein Unternehmen setzt flächendeckend Fingerabdrucksensoren zur Zutrittskontrolle für bestimmte Bereiche ein.

Quelle: Version 1.1. vom 17.10.2018

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)

- Was ist Bestandteil einer datenschutzrechtlichen Dokumentation (Empfehlung)?
 - Verarbeitungsverzeichnis mit der Dokumentation (TOM's)
 - Datenschutzfolgeabschätzung (DSFA)
 - Verträge
 - Ethikvotum
 - Patienten-Informationen und -Einwilligungen.

Vielen Dank für Ihre Aufmerksamkeit.....