

PrivacySoft – Eine Einführung für Verantwortliche

Wolfgang Rottwinkel
Behördlicher Datenschutzbeauftragter



Die Grundlage

Art. 4 Nr. 1 DSGVO

- „personenbezogene Daten“ [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

Warum das Ganze?

Gesetzliche Vorgabe seit dem 25.05.2018

- **Art. 30 I DSGVO:**
Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen
- **Verantwortlicher:**
Präsidium (§ 37 I NHG) unter Führung des Präsidenten (§ 38 I NHG)
- **Datenschutzrichtlinie der TiHo vom 24. September 2018:**
Die datenschutzrechtlich Verantwortlichen sind die Leitungen der jeweiligen Dezernate der Hochschulverwaltung, Stabsstellenleitungen des Präsidiums, die jeweiligen Klinik- und Institutsleitungen und die Leitungen anderer Hochschulreinrichtungen

Warum PrivacySoft?

Effektivität & Rechtssicherheit

- **Art. 30 III DSGVO:**
Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann
- **Art. 30 IV DSGVO**
Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung
- **Aufgabe des DSB, Art. 39 DSGVO**
auch: Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften (...) für den Schutz personenbezogener Daten

Anmeldung in PrivacySoft

<https://privacysoft.online>

- Mandant: 344
- Anmeldename: i.d.R. Ihre IDM#
- Passwort: das kennen bitte nur Sie!

Anmeldemaske PrivacySoft

Startbildschirm

Die einzelnen Menüpunkte

- ALL: Komplette Übersicht über die für Sie freigeschalteten Vorgänge
- ACC: Nachweispflichtenübersicht
- **VVV: Verzeichnis der Verarbeitungstätigkeiten**
- **TOM: Technisch und organisatorische Maßnahmen**
- AV: Auftragsverarbeitungsverträge
- VOR: Vorgänge
- SUB: Meldungen (von Datenpannen)
- DOK: hilfreiche Kurzpapiere



Menüpunkte

Für uns besonders wichtig: VVV!



Kopfbereich

Verzeichnis der Verarbeitungstätigkeiten

- NEU: Neue Verarbeitungstätigkeit erstellen
- Archivierte: Archivierte VA betrachten
- DSFA: Datenschutzfolgeabschätzung
 - wird von DSB/DSK vorgenommen
 - Art. 35 I DSGVO (Hat eine Form der Verarbeitung (...) ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der (...) für den Schutz personenbezogener Daten durch.
- Detailansicht / Optionsmenü 
- Darunter: Ihre Verarbeitungstätigkeiten

Verarbeitungstätigkeit

Was ist eine Verarbeitungstätigkeit?

- **Art. 4 Nr. 2 DSGVO**

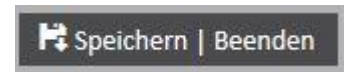
Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche **Vorgangsreihe** im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

Neue Verarbeitungstätigkeit anlegen



Los geht's....

- Klick auf „Neu“
- Art der Neuanlage ist i.d.R. eine „Neuanlage per Vorlage“, anders wäre es nur, wenn Sie eine oder mehrere VA kopieren wollen (dann, wenn Ihre Verarbeitungstätigkeiten sehr, sehr ähnlich sind)
- Freigabestatus „In Planung“, wird von DSB/DSK freigegeben
- Gültigkeit immer bei einem Jahr belassen
- Bezeichnung frei wählbar
- Zugeordnete Abteilung: Ihre OE
- Zuständiger Kontakt: OE-Leiter/in



Beginn der Bearbeitung

Daten noch einmal kontrollieren

Bezeichnung:	Warum Datenschutz so viel Spaß macht...!	Bewertung:	
Unternehmen:	Stiftung Tierärztliche Hochschule Hannover	Freigabestatus:	In Planung
Abteilung:	Datenschutz	Vorlage:	DSGVO Verarbeitun...
Zuständig:	Wolfgang Rottwinkel	Ersteller:	Wolfgang Rottwi...
Gültig bis:	04.02.2020	Gültig ab:	04.02.2019
Schlagwörter			

Gemeinsame Verantwortliche



Verknüpfungen (0)

Verknüpfen 



- Gemeinsame Verantwortliche: Falls mehrere Personen für denselben Verarbeitungsvorgang verantwortlich sind, können diese hier hinterlegt werden
- Unter „Verknüpfen“ können passende Verträge (bspw. AVV gem. Art. 28 oder gemeinsame Verantw. gem. Art. 26 DSGVO) an die VA geknüpft werden

12 Fragen zum Erfolg

#1 Beschreibung der Verarbeitungstätigkeit

- Hier beschreiben Sie Ihre Verarbeitungstätigkeit bzw. Ihre **Vorgangsreihe**
- Bitte beschreiben Sie knapp was mit den Daten passiert oder wie Sie diese verarbeiten
- Beispiel: **Elektronische Aktenführung** von Patientenbesitzern mittels der **Software** easyVet *oder* Anlage einer **papierbasierten** Personalakte

#2 Zweck der Verarbeitung

- Wichtig: Wozu verarbeiten Sie die Daten?
- Sie sollten sich einen Verarbeitungszweck aus dem Drop-Down-Menü aussuchen; dennoch muss im Textfeld der **Zweck näher beschrieben** werden
- Beispiel: **Beschäftigungsverhältnis**
Die Anlage einer Personalakte dient der leichten Auffindbarkeit aller Daten der/des Beschäftigten; darüber hinaus dient sie der Erfüllung gesetzlicher Anforderungen

#3 Rechtsgrundlage der Verarbeitung

Verarbeitung von personenbezogenen Daten muss stets auf einer Rechtsgrundlage beruhen (Verbot mit Erlaubnisvorbehalt).

Passende Rechtsnorm ist im Freitextfeld zu ergänzen!

Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7)

Einwilligung eines Kindes (Art. 6 Abs. 1 lit. a, Art. 8)

Vertrag oder Vertragsanbahnung (Art. 6 Abs. 1 lit. b)

Für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung (Art. 6 Abs. 1 lit. e)

→ **Hier wird dann eine weitere nationale Rechtsnorm benötigt (NBG, NHG, NArchG, NDSG...)**

Wahrung berechtigter Interessen des Verantwortlichen oder des Dritten (Art. 6 Abs. 1 lit. f)

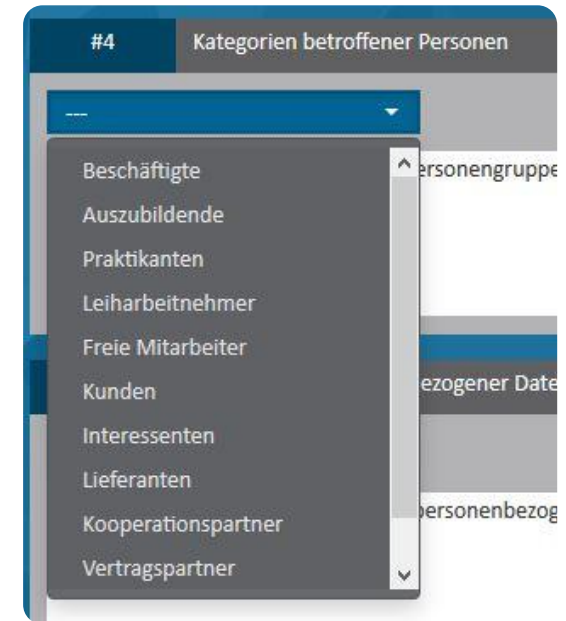
→ **Buchstabe f (wohl) nicht anwendbar für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung**

Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs.)

Wissenschaft und Forschung (Art. 89 DSGVO i.V.m. § 13 NDSG)

#4 Kategorien betroffener Personen

- (Mehrfach-)Auswahl aus dem Drop-Down-Menü
- Als betroffene Personengruppen kommen beispielsweise Kunden, Auftraggeber, Interessenten, Mandanten, Patienten, Arbeitgeber, Mitarbeiter, Bewerber, Mieter, Lieferanten usw. in Betracht
- Bei der Auswahl von „Sonstige“ müssen diese im Textfeld näher ausgeführt werden



#5 Kategorien personenbezogener Daten

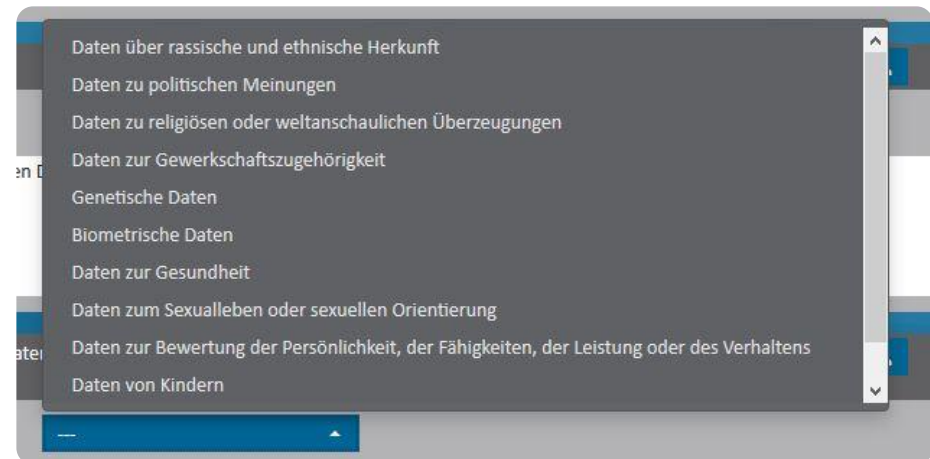
- Auswahl (einer oder mehrerer) Optionen aus dem Drop-Down-Menü

- Zusätzliche Angaben im Textfeld:

Abrechnungsdaten, Adressdaten, Bankverbindungsdaten / Kreditkartendaten, Bonitätsdaten, Geburtsdatum, IT-Nutzungsdaten / Log Daten / Protokolldateien, IP-Adresse, Interessen / Präferenzen, Kontaktdaten, Lohn- und Gehaltsdaten, Lebenslauf, Name/Vorname/Anrede/Titel, Qualifikationsdaten / Leistungs- und/oder Potenzialbeurteilung, Sozialversicherungsdaten, Standortdaten, Vertragsdaten, Vertragsstammdaten, Zahlungsdaten, Zeiterfassungsdaten...

#6 Besondere Kategorien personenbezogener Daten

- Auswahl einer oder mehrerer Kategorien aus dem Drop-Down-Menü
- i.d.R. nicht einschlägig
 - Ausnahme: Personalverwaltung, Betriebsarzt, Personalrat....
- Begriff des Kindes:
Nichtvollendung des **16. Lebensjahres**



#7 Rechtsgrundlage bei der Verarbeitung besonderer Kategorien

- Sollten personenbezogene Daten besonderer Kategorien verarbeitet werden, ist besonders auf die Rechtsgrundlage zu achten, da die DSGVO **keinen Spielraum** zulässt
- Rechtsgrundlage im Drop-Down-Menü auswählen und die konkrete(n) Norm(en) im Freitextfeld ergänzen
- Bei **behördlichem Handeln** i.d.R.:
Art. 6 Abs. 1 lit. e DSGVO i.V.m.
niedersächsischem / deutschem Recht

#7 Falls besondere personenbezogene Daten erhoben werden, nennen Sie bitte die Rechtsgrundlage der Verarbeitung.

Rechtsgrundlagen erfolgen

- Einwilligung des Betroffenen
- Arbeitsrecht, Recht der sozialen Sicherheit, Sozialschutz, Kollektivvereinbarung
- Schutz lebenswichtiger Interessen
- Mitgliederdaten von Stiftungen, Vereinigungen oder Organisationen
- Verarbeitung ist von der betroffenen Person öffentlich zugänglich gemacht worden
- Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- Erhebliches öffentliches Interesse
- Arbeitsmedizinische Untersuchung, Gesundheitsvorsorge
- Patientenversorgung, Untersuchung/Impfung durch Ämter
- Wissenschaftliche/historische Forschung/Archivierung

#8 Herkunft der Daten

- Tragen Sie hier ein, woher die Daten stammen
- Beispiele:
 - von der betroffenen Person selbst
 - von kooperierenden Tierarztpraxen
 - von anderen öffentlichen Stellen
 - aus dem Internet
 - vom Hausarzt
 - ...

#9 Weitergabe an Dritte?

- „Dritter“ [ist] eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten, Art. 4 Nr. 10 DSGVO
- Bitte hier im Drop-Down auswählen und im Freitext konkretisieren
- Insbesondere sind auch **andere OE anzugeben**, an die die Daten ggf. weitergegeben werden

#9 Werden personenbezogene Daten an Dritte weitergegeben? Wenn ja, aus welchen Empfängern?

- Externer Dienstleister / Auftragsverarbeiter (bitte angeben)
- Externer Dienstleister / Funktionsübertragung (bitte angeben)
- Anderes Unternehmen / Übermittlung (bitte angeben)
- Andere Abteilung (bitte angeben)
- Andere Konzerngesellschaft (bitte angeben)
- Empfänger außerhalb der EU/EWR (bitte angeben / Garantien notwendig)

Bitte geben Sie an, welche Anwendungen (Software, Datenbanken, Cloud-Anwendungen) ur

#10 Beteiligten Anwendungen und Systeme

#10

Beteiligte Anwendungen und Systeme

Anlage

Bitte geben Sie an, welche Anwendungen (Software, Datenbanken, Cloud-Anwendungen) und / oder Systeme (Hardware) an der Verarbeitung beteiligt sind.

- Tragen Sie hier ein, welche Soft- und Hardware Sie benutzen
- Software (SAP, easyVet, LabControl, etc.)
- Hardware (PC, Laptop, Tablet, etc.)
- Cloud-Dienste
- Datenbanken

#11 Lösch- und Aufbewahrungsfristen

#11 Lösch- und Aufbewahrungsfristen / Löschkonzept Anlage

Gibt es Angaben zu Lösch- bzw. Aufbewahrungsfristen? Führen Sie bitte ggf. vorhandene Löschkonzepte auf.

- Machen Sie an dieser Stelle deutlich, wie lange Sie die Daten aufbewahren bzw. speichern.
- Begründen Sie, warum Sie Daten wie o.a. aufbewahren und speichern
- Machen Sie Angaben, **wie** Sie die Daten löschen
- Sofern Sie einer (**rechtlichen**) **Aufbewahrungspflicht** unterliegen, geben Sie sie hier an

#12 Datensicherheit / TOM

- Drop-Down-Menü für die TiHo **nicht passend**, daher an dieser Stelle nichts auswählen
- Alle Verarbeitungstätigkeiten werden mit den „allgemeinen TOMs“ für die TiHo verknüpft
- Sofern Sie besondere Software oder Hardware nutzen, bedarf es hierzu zusätzlicher Informationen.
- Beispiel: **easyVet** wird besonders gesichert, da nur bestimmte IP-Adressen und Standorte Zugriff haben; dies ist hier entsprechend aufzuführen. Ebenso ist aufzuführen, dass für den **SAP-Zugang** eine personifizierte Zugangskarte erforderlich ist, etc.
- Nicht aufgezählt werden muss, dass Sie Ihren Rechner sperren (**Windows + L**) und die **Tür abschließen**, wenn Sie das Büro verlassen, da dies TiHo-weit gilt.

#13 Datenschutzfolgeabschätzung

- Sollte Ihnen #13 angezeigt werden, müssen (und dürfen) Sie hier nichts ausfüllen. Das übernehmen DSB/DSK für Sie
- Ggf. kommen wir auf Sie zu, um etwaige Unklarheiten zu beseitigen und das Risiko eines Datenschutzvorfalls zu mindern

#13

Beurteilung des Datenschutz-Risikos

Anlage

„Muss-Liste“ (Blacklist) der deutschen Datenschutzaufsichtsbehörden

Einsatzfeld

☐ Betrieb eines Insolvenzverzeichnisses

- Träger von großen sozialen Einrichtungen
- Große Anwaltssozietät

☐ Fahrzeugdatenverarbeitung – Car-sharing / Mobilitätsdienste.

- Fahrzeugdatenverarbeitung – Zentralisierte Verarbeitung der Messwerte oder Bilderzeugnisse von Umgebungsensoren.
- Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o.ä.
- Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes

Beschreibung

Beispiel

Risikoeinschätzung:

Eintritt: | Schwere:

Akzeptabel

41	42	43	44
31	32	33	34
21	22	23	24
11	12	13	14

Schweregrad →

Eintrittswahrscheinlichkeit →

Bitte bestimmen Sie hier das Risiko.
Das Risiko soll nach objektiven Kriterien ermittelt werden.
Die Faktoren sollen Art, Umfang, Umstände und Zweck einer konkreten Verarbeitung berücksichtigen.

Hierzu bedarf es der Einstufung nach zweierlei Kriterien:

1. Schwere des Schadens auf der vertikalen Achse und
2. Eintrittswahrscheinlichkeit auf der horizontalen Achse.

Auf jeder Achse lassen sich dabei vier verschiedene Wirkungsgrade abbilden:

- Vernachlässigbar (1)
- Begrenzt (2)
- Wesentlich (3)
- Maximal (4)

Die Relation von Schaden und Eintrittswahrscheinlichkeit bestimmt somit das Risiko:

- **akzeptabel** (grün)
- so niedrig wie möglich → **Risikoreduktion** (gelb)
- **INAKZEPTABEL** (rot)

Anlagen hinzufügen

- Sie haben zu jeder Frage, die Möglichkeit, eine Anlage hinzuzufügen
- Dies bietet sich an, wenn Sie Excel-Listen, Word-Dokumente, Bildschirmabdrücke, PDFs, etc. auf Ihrem Rechner haben, die die Beantwortung einer Frage sinnvoll ergänzen können
- Klicken Sie dazu innerhalb der Frage rechts auf „Anlage“, durchsuchen Sie Ihren Rechner nach dem jeweiligen Dokument und laden Sie es hoch
- Für Dokumente, die den gesamten Verarbeitungsvorgang betreffen, klicken Sie vor der ersten Frage auf „Verknüpfen“ und verfahren, wie oben beschrieben. Verknüpfungen sind i.d.R. Verträge und/oder andere Vereinbarungen

Verknüpfungen (0)

Verknüpfen  

Eine Verarbeitungstätigkeit bearbeiten

- Sie haben auch die Möglichkeit, bereits vorhandene Verarbeitungstätigkeiten zu bearbeiten, sofern sich ein Verfahren ändert
- Klicken Sie dazu auf  im oberen rechten Bereich Ihrer Verarbeitungstätigkeit. Dort lassen sich die Strukturdaten (Bezeichnung, Abteilung, Gültigkeit, etc.) anpassen
- Wollen Sie die Antworten auf die zwölf Fragen bearbeiten, öffnen Sie Ihre Verarbeitungstätigkeiten und bearbeiten Sie Ihre Antworten direkt in den Feldern
- Verarbeitungstätigkeiten können nur archiviert aber nicht gelöscht werden!



Für Rückfragen stehe ich Ihnen jederzeit zur Verfügung!
Herzlichen Dank für Ihr Interesse.

Wolfgang Rottwinkel
Behördlicher Datenschutzbeauftragter