Stiftung Tierärztliche Hochschule Hannover
University of Veterinary Medicine Hannover

Erläuterungen zum Umgang mit der Datenschutzrichtlinie der Stiftung Tierärztliche Hochschule Hannover vom 24.09.2018

Geltungsbereich:	Alle Bereiche der Hochschule
Version/ Datum der Herausgabe:	11.08.2021
Erstellt durch:	Behördlicher Datenschutzbeauftragter (DSB)

Zu § 1 – Sachliche und räumliche Zuständigkeit

I. Die Datenschutzrichtlinie der TiHo dient dem Schutz der personenbezogenen Daten und der Umsetzung der Datenschutz-Grundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG) sowie des Niedersächsischen Datenschutzgesetzes (NDSG).

II. Die TiHo ist eine öffentliche Stelle des Landes Niedersachsen, sodass die Regelungen der niedersächsischen Gesetze, sofern welche vorhanden sind, den Regelungen der DSGVO vorgehen, bzw. die DSGVO ergänzen können (**zum Beispiel**: NDSG, NHG)

Rechtsgrundlage:
Die sachliche und räumliche Zuständigkeit ist geregelt in Art. 1 und Art. 2 DSGVO

Wichtig:
Nur der erste und der dritte Teil des NDSG findet Anwendung bzgl. der DSGVO, der zweite Teil ist für den Datenschutz an der TiHo nicht relevant.

Zu § 2 – Begriffsbestimmungen

I. Die DSGVO hat das Ziel, personenbezogene Daten zu schützen. Dazu gibt sie den Betroffenen Rechte an die Hand.
Jede betroffene Person soll eine feste Ansprechperson haben, an die sie sich wenden kann. Dies ist die **verantwortliche Person**.

II. Damit alle Begrifflichkeiten für jedermann klar sind, hat sich die DSGVO entschieden, diese zu definieren. Diese Definitionen sind europaweit gleich und helfen, die Inhalte der DSGVO besser zu verstehen.

Weitere Informationen:
Die Rechte der Betroffenen sind in Artt. 12 ff. DSGVO geregelt. Die Grundsätze für die Verarbeitung regelt Art. 5 DSGVO.

Weitere Definitionen lassen sich aus Art. 4 DSGVO entnehmen.

Zu § 3 – Verantwortliche

I. In den Einrichtungen handeln die jeweiligen Leitungen eigenverantwortlich und entscheiden darüber, wie die Datenverarbeitung umgesetzt wird. Damit werden die jeweiligen Leitungen zu Verantwortlichen.

II. Die verantwortliche Person entscheidet **zum Beispiel**, ob eine Akte angelegt werden muss, wie Patienten kontaktiert werden sollen, wie die Kommunikation in der Einrichtung organisiert wird oder ob Dienstpläne ausgehängt werden.

III. Um die Verantwortlichen zu entlasten, können sie eine/n dezentrale/n Datenschutz-Koordinator/in **(dDSK)** benennen, um die Vorgaben aus der DSGVO in der jeweiligen Einrichtung umzusetzen. Jede/r dDSK dient als Ansprechpartner/in für den/die behördliche/n Datenschutzbeauftragte/n **(DSB)**.

Rechtsgrundlage:
Der Begriff „Verantwortlicher“ ist definiert in Art. 4 Nr. 7 DSGVO.

Nähere Informationen:
Die Idee dahinter ist, dass ein stetiger Austausch zwischen den Einrichtungen und der zentralen Verwaltung stattfinden kann. DSB/DSK stehen daher für Beratung und Hinweise stets zur Verfügung.

Zu § 4 – Grundsätze

I. Die DSGVO stellt die Grundsätze zur Verarbeitung von personenbezogenen Daten selbst sehr ausführlich dar. Das zentrale Element dabei ist das **Verbot mit Erlaubnisvorbehalt**. Die Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten, es sei denn, sie ist erlaubt.

II. Die weiteren Grundsätze der Verarbeitung sind in der DSGVO direkt geregelt. In diesem Falle lässt sich die DSGVO als „Nachschlagewerk“ nutzen.

III. Die wichtigsten Auswirkungen des Art. 5 DSGVO sollen hier kurz dargestellt werden:

a. Für betroffene Personen soll jeder einzelne Schritt der Datenverarbeitung klar und verständlich sein, Mitteilungen zum Datenschutz sollen leicht zugänglich und in klarer und einfacher Sprache verfasst sein. Für die TiHo bedeutet dies **zum Beispiel**, dass Hinweise zum Datenschutz auf der Internetseite der Einrichtung oder beim Ausfüllen von Formularen, Umfragen, etc. vorhanden sind.

Hinweis:
Erlaubt ist die Verarbeitung nur, wenn eine Rechtsgrundlage **oder** eine Einwilligung der betroffenen Person vorliegt!

Rechtsgrundlage:
Art. 5 DSGVO

b. Ebenso muss den betroffenen Personen der **Zweck** der Datenverarbeitung deutlich gemacht werden. Dies kann direkt mit den Hinweisen zum Datenschutz kombiniert werden. Die verantwortlichen Personen müssen außerdem darauf achten, nur diejenigen Daten zu verarbeiten, die für den angedachten Zweck wirklich **notwendig** sind. Es muss beispielsweise darauf verzichtet werden, bei der Anlage einer Patientenakte nach der Religionszugehörigkeit zu fragen.

Hinweis:
Natürlich darf nach dem Geburtsdatum gefragt werden, um zu schauen, ob jemand bereits vollumfänglich Verträge abschließen darf. Name, Adresse und ggf. Bankverbindung sind für die Rechnungstellung ebenfalls notwendig.

c. **Wichtig** für die TiHo ist, dass vom Grundsatz der Zweckbindung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke abgewichen werden kann.

Rechtsgrundlage:
Art. 5 Abs. 1 DSGVO, § 13 NDSG

d. Beim **Verbot mit Erlaubnisvorbehalt** kommt es also darauf an, entweder eine Einwilligung zu erhalten oder eine Rechtsgrundlage zu finden, die die Verarbeitung gestattet. Der bevorzugte Weg sollte dabei das **Auffinden einer Rechtsgrundlage** sein, da dies den administrativen Aufwand deutlich reduziert.

Besser: Rechtsgrundlage finden
Das liegt daran, dass bei einer Einwilligung eine Unterschrift oder das Anklicken eines Häkchens im Online-Formular notwendig ist. Die TiHo muss dann zum Nachweis diese Dokumente vorrätig halten. Das führt zu mehr digitalen oder händischen Akten. Bei Vorliegen einer Rechtsgrundlage genügt eine Information zum Datenschutz.

e. Liegt eine Rechtsgrundlage nicht vor, muss die betroffene Person in die Datenverarbeitung **einwilligen**. Dazu bedarf es einer schriftlichen (durch Unterschrift) oder einer digitalen Erklärung. Die schriftliche Erklärung muss also ein Formular sein, auf dem sich die betroffene Person ausdrücklich dazu bereit erklärt, ihre Daten für den angegebenen Zweck zur Verfügung zu stellen. Im Online-Bereich genügt das Anklicken eines Kästchens. **Entscheidend** für die rechtskonforme Einwilligung ist, dass den betroffenen Personen alle entscheidungsrelevanten Informationen zur Verfügung gestellt werden. Die Verantwortlichen müssen **nachweisen** können, dass eine Einwilligung eingeholt wurde.

Hinweis:
Laut DSGVO genügt auch eine **mündliche** Einwilligung. Diese wird aber im Streitfall schwer zu beweisen sein!

Rechtsgrundlage der Einwilligung:
Art. 6 Abs. 1 Buchstabe a DSGVO

Zu § 5 – Rechte der Betroffenen

I. Die Verantwortlichen müssen die Rechte der betroffenen Personen sicherstellen. Es bleibt bei dem zentralen Element, dass die Betroffenen immer darüber informiert werden müssen, wozu die Daten verarbeitet werden und wer die verantwortliche Person ist. Vor oder bei der Verarbeitung der Daten müssen daher mindestens folgende Informationen mitgeteilt werden: den Namen und die Kontaktdaten der verantwortlichen Person, die Kontaktdaten der oder des DSB, die Zwecke der Verarbeitung, die Rechte der betroffenen Person und dabei insbesondere das Recht auf Widerruf (sofern die Verarbeitung auf einer Einwilligung beruht), die Möglichkeit der Beschwerde bei der Aufsichtsbehörde sowie – sofern passend – die Rechtsgrundlage der Verarbeitung.

Rechtsgrundlage:
Art. 13 DSGVO

In der Praxis:
Die TiHo stellt diese Informationen entweder auf der Einwilligungserklärung oder den Informationen zum Datenschutz zur Verfügung, wenn keine Einwilligung notwendig ist – dies ist sowohl online als auch in Papierform möglich.

II. Die oben genannten Informationspflichten sollten nicht zu streng gesehen werden. Viele der Punkte ergeben sich bereits aus dem Kontext des Formulars – **zum Beispiel**, wenn eine Person an einer Umfrage teilnimmt, die eine gewisse Überschrift hat, ist ihr der Zweck bereits deutlich gemacht. Auch muss auf die Rechte aus der DSGVO nicht explizit hingewiesen werden.

Hinweis:
Es würde hier genügen mitzuteilen, dass die Verarbeitung auf Grundlage der DSGVO erfolgt. Eine Aufzählung aller Rechte ist nicht nötig.

III. Ein weiteres Recht von Betroffenen ist das Recht auf **Auskunft**. Das Auskunftsrecht geht genauso weit, wie das Recht auf Informationen, das oben bereits beschrieben ist. Natürlich hat die betroffene Person auch das Recht, unrichtige Daten **korrigieren** zu lassen.

IV. Besonders **wichtig** ist das Recht auf **Löschung**. Dies besteht nur, wenn die Zwecke für die Verarbeitung nicht mehr vorliegen oder eine erklärte Einwilligung widerrufen wurde und keine andere Rechtsgrundlage mehr zur Verfügung steht. Die Verantwortlichen müssen dann sicherstellen, dass alle Daten der betroffenen Person datenschutzsicher gelöscht werden.

Hinweis:
Sind Daten bereits öffentlich gemacht (bspw. in Printmedien) ist eine Löschung nicht mehr möglich und damit auch nicht notwendig. Auch ist die Löschung bei **Ausnahmen** nach Art. 17 Abs. 3 DSGVO nicht möglich.

V. **Weitere Rechte** ergeben sich aus Artt. 18, 20 und 21 DSGVO.

Zu § 6 – Technisch und organisatorische Maßnahmen

I. Die technischen und organisatorischen Maßnahmen (TOMs) dienen insbesondere der **Datensicherheit**. Systemseitig trifft das Dezernat Informations- und Datenverarbeitungsservice (IDS) die grundsätzlichen TOMs. Dennoch muss jede verantwortliche Stelle darüber hinaus **eigene TOMs** entwickeln, die auf ihre besonderen Formen der Datenverarbeitung angepasst sind. Dies kann **beispielsweise** dadurch erfolgen, dass Büroräume beim Verlassen stets abgeschlossen werden, Akten nicht offen in Büros ausliegen, Aktenschränke stets verschlossen sind, eine Abmeldung vom PC bei Verlassen des Raumes vorgenommen wird, etc.

II. Die TOMs sind von den Verantwortlichen vollständig zu dokumentieren und innerhalb eines Verzeichnisses zu führen. Das Verzeichnis der TOMs wird mittels einer **zentralen Softwarelösung** (derzeit *PrivacySoft*) geführt. Die verantwortliche Person erhält Zugang zu dieser Software durch Anmeldung beim IDS. Zentrales Element der TOMs ist deren **Vollständigkeit**. Jeder Form der Verarbeitung von personenbezogenen Daten muss eine oder müssen mehrere eigene TOM(s) gegenüberstehen.

Hinweis:
Die Nutzung der Software wird in regelmäßigen Schulungen erläutert.

III. In der Praxis bedeutet das, dass sich die Verantwortlichen Gedanken machen müssen, welche **Verarbeitungsvorgänge** in ihrer Einrichtung stattfinden. Bestenfalls werden passende Sicherheitsmaßnahmen in die Überlegungen einbezogen und dann direkt in die Software eingetragen.

Zu § 7 – Verzeichnis der Verarbeitungstätigkeiten

I. Zur Führung des zwingend vorgeschriebenen Verzeichnisses der Verarbeitungstätigkeiten nutzt die TiHo ebenfalls eine zentrale Software-Lösung (derzeit *PrivacySoft*). Die verantwortliche Person erhält Zugang zu dieser Software durch Anmeldung beim IDS.

Rechtsgrundlage:
Art. 30 Abs. 1 DSGVO

II. Jede verantwortliche Stelle muss für jeden einzelnen Verarbeitungsvorgang eine Beschreibung erstellen. Dabei ist darauf zu achten, einen Vorgang **so allgemein wie möglich aber so genau wie nötig** zu beschreiben. **Beispiel:** Es ist nicht nötig, bei der Anlage einer Kundenakte bei der Annahme eines neuen Patienten für jedes einzelne Datum (Name, Anschrift, Telefonnummer des Besitzers) einen eigenen Verarbeitungsvorgang zu beschreiben; vielmehr ist es aber notwendig das Verfahren „Anlage einer Kundenakte“ anzulegen. Ebenso verhält es sich bei Verfahren zum „Aushang eines Dienstplans“, usw. Auch bedarf es bspw. bei Neueinstellungen nicht für jeden Verarbeitungsvorgang einer eigenen Beschreibung; es genügt, sämtliche Verarbeitungsschritte im Vorgang „Neueinstellung“ festzulegen.

Hinweis:
Auch hier kommt es auf die Vollständigkeit und die Aktualität des Verzeichnisses an!

III. **Bestenfalls** ist jede Verarbeitungstätigkeit direkt mit einer TOM **verknüpft**.

Zu § 8 – Vorgehen bei Datenschutzvorfällen

I. Ein Datenschutzvorfall ist eine Unregelmäßigkeit in der Verarbeitung personenbezogener Daten, die zu einem Risiko der betroffenen Person geführt hat oder führt.

II. Liegt der Verdacht auf einen Datenschutzvorfall vor oder ist dieser bereits eingetreten, haben die Verantwortlichen gemeinsam mit DSB 72 Stunden Zeit, diesen bei der Aufsichtsbehörde zu melden. Eine verspätete Meldung bedarf einer Begründung, sodass zügiges und sicheres Verhalten notwendig ist.

Hinweis:
Nicht jeder Vorfall muss gemeldet werden. Die Entscheidung treffen die Verantwortlichen nach Rücksprache mit DSB.

Rechtsgrundlage:
Art. 33 DSGVO

Folgende Schritte sind zu unternehmen:

a. Zügige Meldung: Hat eine (verantwortliche) Person den Verdacht, dass ein Datenschutzvorfall vorliegt, so wird der DSB **unverzüglich** unterrichtet. Dabei sind folgende Informationen zu melden: Detaillierte Sachverhaltsschilderung, wer ist Verantwortlicher, Zeitraum oder Zeitpunkt des Vorfalls, Zeitpunkt der Feststellung des Vorfalls, Ursache des Vorfalls, Ort des Vorfalls, Art der Verletzung, Kategorien der betroffenen Personen, Anzahlen der betroffenen Personen, Kategorien der personenbezogenen Daten (insbesondere Art. 9 DSGVO), Zweck der Verarbeitung, mögliche Folgen und Auswirkungen für die betroffene Person.

Hinweis:
Die Meldung des Vorfalls kann formlos via E-Mail erfolgen.

b. Im Anschluss an die Meldung nimmt der DSB eine Bewertung der Intensität des Vorfalls vor; als Hinweis hierzu dienen insbesondere die Kategorien der personenbezogenen Daten, die verletzt sein könnten.

c. Der DSB berät die verantwortliche Stelle im Anschluss an die Bewertung zu geeigneten Gegenmaßnahmen. Hierbei wird auf die gesammelten Erfahrungen bei vergangenen Vorfällen zurückgegriffen. Abschließend entscheiden die verantwortlichen Personen – nach Beratung mit DSB/DSK – wie weiter vorgegangen werden sollte.

Kontakt zum behördlichen Datenschutzbeauftragten

Behördlicher Datenschutzbeauftragter

Wolfgang Rottwinkel
TiHo-Tower, Raum 916
Tel.: 8014 & 8015
Fax: 828014

wolfgang.rottwinkel@tiho-hannover.de

Alternative E-Mail-Adresse

datenschutz@tiho-hannover.de