



„Datenschutzrichtlinie“

Richtlinie zur Einhaltung datenschutzrechtlicher Grundsätze an der Stiftung Tierärztliche Hochschule Hannover

Geltungsbereich:

Alle Bereiche der Hochschule

Datum der Verabschiedung

24.09.2018

Erstellt durch:

Datenschutz-Koordinator (DSK)

Freigabe durch:

Präsidium

§ 1

Sachliche und räumliche Zuständigkeit

Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten und entfaltet ihre Gültigkeit in allen Bereichen der Stiftung Tierärztliche Hochschule Hannover.

§ 2

Begriffsbestimmungen

Im Sinne der Datenschutz-Grundverordnung (DSGVO) bezeichnet der Ausdruck

- „personenbezogene Daten“ 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;
- „Verarbeitung“ jeden 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;
- „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

§ 3

Verantwortliche

1. Die datenschutzrechtlich Verantwortlichen sind die Leitungen der jeweiligen Dezernate der Hochschulverwaltung, Stabsstellenleitungen des Präsidiums, die jeweiligen Klinik- und Institutsleitungen und die Leitungen anderer Hochschulreinrichtungen.
2. Soweit die Verarbeitung personenbezogener Daten in zentral betreuten Systemen erfolgt (zum Beispiel easyvet, Labcontrol oder MyTMA), geht die systemseitige Verantwortung für den Datenschutz auf die jeweiligen Leitungen der Dezernate der Hochschulverwaltung über.
3. Die dezentral Verantwortlichen haben das Recht, dezentrale Datenschutz-Koordinatoren für den eigenen Verantwortungsbereich zu benennen, welche als Ansprechpersonen für den behördlichen Datenschutzbeauftragten oder die behördliche Datenschutzbeauftragte (DSB)

und den zentralen Datenschutz-Koordinator oder die zentrale Datenschutz-Koordinatorin (DSK) dienen und die Aufgaben der jeweiligen Verantwortlichen übernehmen können. Die Benennung von dezentralen Datenschutz-Koordinatoren und -koordinatorinnen entbindet die Verantwortlichen nicht von deren Pflichten.

§ 4 **Grundsätze**

Die Grundsätze der DSGVO bei der Verarbeitung personenbezogener Daten sind einzuhalten. Diese sind die Rechtmäßigkeit der Verarbeitung, die Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit der Datenverarbeitung, Speicherbegrenzung sowie Integrität und Vertraulichkeit.

§ 5 **Rechte der Betroffenen**

Die Sicherstellung der Betroffenenrechte obliegt den Verantwortlichen. Dies sind insbesondere die Informationspflichten, das Auskunftsrecht, das Recht auf Berichtigung, das Recht auf Löschung, das Recht auf Einschränkung der Verarbeitung, das Recht auf Datenübertragbarkeit sowie das Widerspruchsrecht.

§ 6 **Technisch und organisatorische Maßnahmen**

Die Sicherstellung des Datenschutzes erfordert neben einem verantwortungsvollen Umgang mit den materiellen Anforderungen innerhalb der datenverarbeitenden Stelle auch die Verwendung einer sicheren, gegen Eingriffe von Nichtberechtigten gesicherten Infrastruktur. Das Dezernat Informations- und Datenverarbeitungsservice (IDS) trifft grundsätzliche technische und organisatorische Maßnahmen (TOMs), um das von der TiHo benötigte Maß an Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Aus Sicht des Datenschutzes sind die Maßnahmen des IDS als wesentliches Werkzeug zur Erreichung der Datenschutzziele zu betrachten.

§ 7 **Verzeichnis der Verarbeitungstätigkeiten**

Die jeweiligen Verantwortlichen sind dazu verpflichtet, ein schriftlich geführtes Verzeichnis für die Verarbeitungstätigkeiten zu führen, die deren Zuständigkeit unterliegen. Die TiHo bedient sich zur Erstellung, Führung und Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten einer zentralen Softwarelösung.

Die jeweiligen Verzeichnisse werden durch den oder die DSB/DSK einer inhaltlichen Überprüfung unterzogen und freigegeben, sobald diese den Nachweispflichten nach der DSGVO entsprechen. Abweichungen von diesem Verfahren sind nur nach Absprache mit dem oder der DSB/DSK zulässig.

§ 8
Vorgehen bei Datenschutzvorfällen

Sollten trotz aller Bemühungen Unregelmäßigkeiten bei der Verarbeitung von personenbezogenen Daten auftreten, sind diese unverzüglich der oder dem DSB und/oder DSK mitzuteilen. DSB und/oder DSK nehmen sodann eine Bewertung der Intensität des Vorfalls vor, stimmen mit den Verantwortlichen geeignete Gegenmaßnahmen ab und entscheiden, wie weiter vorzugehen ist.

§ 9
Inkrafttreten

Diese Richtlinie tritt am Tag nach ihrer Veröffentlichung in Kraft.