Stiftung Tierärztliche Hochschule Hannover
University of Veterinary Medicine Hannover, Foundation

Datenschutz in der Tierarztpraxis

Geht das noch auf eine Kuhhaut?

Wolfgang Rottwinkel
Behördlicher Datenschutzbeauftragter

Stiftung Tierärztliche Hochschule Hannover
University of Veterinary Medicine Hannover, Foundation

Begriffe und Definitionen

Art. 4 DSGVO

Wolfgang Rottwinkel
Behördlicher Datenschutzbeauftragter

Personenbezogene Daten

- „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

Verarbeitung

- „Verarbeitung“ [meint] 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

- „Verantwortlicher“ [ist] 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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

Einwilligung

- „Einwilligung“ der betroffenen Person [ist] jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Stiftung Tierärztliche Hochschule Hannover
University of Veterinary Medicine Hannover, Foundation

Rechte der Betroffenen

Pflichten der Verantwortlichen

Wolfgang Rottwinkel
Behördlicher Datenschutzbeauftragter

Verbot mit Erlaubnisvorbehalt

- Die Verarbeitung von personenbezogenen Daten muss stets auf einer passenden Rechtsgrundlage beruhen; liegt eine solche RGL nicht vor, ist die Datenverarbeitung verboten.
- Dazu Erwägungsgrund 40 der DSGVO:

  Damit die Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden, die sich aus dieser Verordnung oder – wann immer in dieser Verordnung darauf Bezug genommen wird – aus dem sonstigen Unionsrecht oder dem Recht der Mitgliedstaaten ergibt (…).
- Art. 6 Abs. 1 DSGVO
  - Einwilligung
  - Vertragsabwicklung / Vertragsanbahnung
  - Erfüllung einer rechtlichen Verpflichtung
  - Schutz lebenswichtiger Interessen der betroffenen Person
  - Öffentliches Interesse oder Ausübung öffentlicher Gewalt
  - Wahrung berechtigter Interessen (Interessenabwägung)

Art. 5 Abs. 1 DSGVO

- Verarbeitung nach Treu und Glauben
- Transparenz
  - Informationsrechte der Betroffenen gegenüber dem Verantwortlichen
  - Erwägungsgrund 39: Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind.
- Zweckbindung
  - Personenbezogene Daten, die rechtmäßig für einen bestimmten Zweck erhoben worden sind, dürfen auch nur für diesen Zweck verarbeitet werden.
- Datenminimierung
  - Nur notwendige personenbezogene Daten dürfen verarbeitet werden.
- Richtigkeit
  - Pflicht des Verantwortlichen, unrichtige Daten zu korrigieren / löschen.

Art. 5 Abs. 1 DSGVO

- Speicherbegrenzung
  - Pflicht, personenbezogene Daten zu löschen oder zu anonymisieren, wenn der Zweck wegfällt und es keine gesetzliche Speicherpflicht gibt.
- Integrität und Vertraulichkeit
  - Personenbezogene Daten sind durch geeignete technische und organisatorische Maßnahmen (TOM) vor dem (unberechtigten) Zugriff durch Dritte zu schützen. Außerdem dürfen personenbezogene Daten nicht unberechtigt gelöscht und/oder verändert werden.
- Rechenschaftspflicht
  - Der Verantwortliche muss die Einhaltung der Verarbeitungsgrundsätze nachweisen können → Beweislast liegt beim Verantwortlichen.

Verantwortung des Verantwortlichen, Art. 24 DSGVO

- Der Verantwortliche trägt die volle Verantwortung für die personenbezogenen Daten.
- Wer die personenbezogenen Daten für einen bestimmten Zweck verarbeitet und über diese Verarbeitung entscheidet, trägt die Verantwortung.
- Die Verantwortung beginnt mit der Erhebung der Daten und endet mit deren Löschung bzw. Anonymisierung.

Technische Ausgestaltung der Verarbeitung, Art. 25 DSGVO

- *Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche (…) technische und organisatorische Maßnahmen (…).*
- data protection by default
  - Durch Voreinstellung sollen nur solche personenbezogene Daten verarbeitet werden können, die für den Zweck erforderlich sind.
- data protection by design
  - Schon bei der Implementierung bzw. Entwicklung einer Verarbeitungstätigkeit sollen alle Grundsätze aus Art. 5 DSGVO Berücksichtigung finden.
- Pseudonymisierung, Verschlüsselung, Wiederherstellbarkeit, Überprüfung der Wirksamkeit von Schutzmaßnahmen, Backup-Strategien, …

Auftragsverarbeitung, Art. 28 DSGVO

- Wird für die eigene Verarbeitung personenbezogener Daten eine dritte Person eingesetzt, so bleibt der Einsetzende Verantwortlicher für die personenbezogenen Daten.
- Dem Verantwortlichen obliegt die Pflicht, sicherzustellen, dass der Auftragnehmer (= der Auftragsverarbeiter) die Vorgaben der DSGVO einhält und einhalten kann.
- Die Grundsätze der Auftragsverarbeitung sind in einem Vertrag festzuhalten.
    - Unterauftragnehmer nur nach Einwilligung des Verantwortlichen
    - Weisungsrecht des Verantwortlichen
    - Meldung von Datenschutzverstößen an den Verantwortlichen
    - Nennung der TOM

Verzeichnis der Verarbeitungstätigkeiten, Art. 30 DSGVO

- Jede Verarbeitungstätigkeit ist in ein Verzeichnis aufzunehmen, in welchem die datenschutzgerechte Verarbeitung dargestellt wird.
- Auf Nachfrage der zuständigen Aufsichtsbehörde muss der Verantwortliche dieses Verzeichnis vorlegen können.
- Beispiele für Verarbeitungstätigkeiten
  - Kontaktanfragen
  - Personalakten
  - Datenbanken
  - Zeiterfassung
  - Heimarbeit
  - Newsletter
  - Foto- und Videoaufnahmen bzw. -aufzeichnungen
- Ausnahmetatbestand in Art. 30 Abs. 5 kaum einschlägig.

Meldung von Datenschutzverstößen

- = Verletzung des Schutzes von personenbezogenen Daten, die voraussichtlich zu einem nicht unerheblichen Risiko für die Rechte und Freiheiten natürlicher Personen führt.
- Unverzügliche und möglichst binnen 72 Stunden zu erfolgende Meldung an die Aufsichtsbehörde.
- Erwägungsgrund 85:

  Eine Verletzung des Schutzes personenbezogener Daten kann – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.
- Bei voraussichtlich hohem Risiko für die Betroffenen: Pflicht zur Benachrichtigung der Betroffenen, Art. 34 DSGVO.
  - Jeweils einzelfallabhängig

Datenschutzfolgeabschätzung / Benennung eines DSB

- In „kleineren“ Tierarztpraxen in der Regel nicht einschlägig.
- DSFA nur notwendig, bei der umfangreichen Verarbeitung von Gesundheitsdaten, strafrechtlich relevanten Daten, Profiling- und Scoring-Daten sowie bei der systematischen Überwachung öffentlicher Bereiche.
- DSB ist nur zu benennen, bei öffentlichen Stellen, wenn die Kerntätigkeit des Verantwortlichen aus Verarbeitungstätigkeiten bestehen, mindestens zehn (20) Personen ständig mit der automatisierten Verarbeitung beschäftigt sind, wenn DSFA notwendigen sind oder wenn der Verantwortliche personenbezogene Daten geschäftsmäßig verarbeiten.

Informationsrecht

- Gemäß Artikel 13 DSGVO ist der Betroffenen sofort bei der Erhebung der Daten über die Verarbeitung zu informieren.
- Verfügt der Betroffene bereits über die Informationen, besteht keine Informationspflicht.
- Informationspflichten
    - Name und Kontaktdaten des Verantwortlichen, Kontaktdaten des DSB, Zweck und Rechtsgrundlage der Verarbeitung, Berechtigte Interessen im Rahmen einer Interessenabwägung, Empfänger von Daten, Übermittlungen an Drittländer oder internationale Organisationen, Dauer der Speicherung, Rechte der Betroffenen, Widerspruchsrechte, Beschwerderecht bei der Aufsichtsbehörde, automatisierte Entscheidungsfindung, mögliche Zweckänderung.

- Art. 14 DSGVO regelt daneben den Fall, dass die Daten nicht bei dem Betroffenen selbst erhoben worden sind.

Auskunftsrecht, Art. 15 DSGVO

- Auskunftspflichten
  - Zweck der Datenverarbeitung, Kategorien der Daten, Empfänger von Daten, Dauer der Speicherung, Recht auf Berichtigung, Löschung und Widerspruch, Beschwerderecht bei der Aufsichtsbehörde, Herkunft der Daten, automatisierte Entscheidungsfindung, Drittlandübermittlung

- Zur Wahrung des Rechts auf Auskunft sind der betroffenen Person die personenbezogenen Daten auf elektronischem oder papierbasiertem Wege zur Verfügung zu stellen.
- Keine Verpflichtung auf Auskunft, wenn das Auskunftsrecht rechtsmissbräuchlich angewandt wird (bspw. durch tägliches Auskunftsersuchen).

Berichtigung und Löschung, Art. 16, 17 DSGVO

- Recht auf Berichtigung muss ohne unangemessene Verzögerung umgesetzt werden.
- Recht auf Vergessenwerden
  - Speicherung nicht mehr notwendig
  - Widerruf der Einwilligung
  - Unrechtmäßige Verarbeitung
  - Rechtspflicht zum Löschen (nach EU-Recht oder nationalem Recht)
- Einschränkung der Verarbeitung
  - Bestreiten der Richtigkeit
  - Unrechtmäßige Verarbeitung
  - Wegfallen des Zwecks der Verarbeitung
  - Widerspruch nach Art. 21 DSGVO
- Mitteilungspflicht des Verantwortlichen gem. Art. 19 DSGVO.
- Daneben: Recht auf Übertragbarkeit gem. Art. 20 DSGVO
  - Personenbezogene Daten müssen auf eine andere Anwendung übertragen werden können

Stiftung Tierärztliche Hochschule Hannover
University of Veterinary Medicine Hannover, Foundation

Die Einwilligung

Und deren Widerruf

Wolfgang Rottwinkel
behördlicher Datenschutzbeauftragter

Voraussetzungen der Einwilligung, Art. 7 Abs. 1 DSGVO

- Freiwillige Entscheidung
  - Nur möglich, wenn die betroffene Person „eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“ (ErwGr 42 DSGVO)
- In informierter Weise
  - Betroffene Person muss wissen, wer der Verantwortliche ist und für welchen Zweck die Daten verarbeitet werden sollen
  - Person muss in die Lage versetzt werden, zu wissen, dass und in welchem Umfang die Einwilligung erteilt wird.
- Bezogen auf einen bestimmten Zweck
- Bezogen auf eine bestimmte Verarbeitung (keine „Generaleinwilligung“)
- Unmissverständlich
  - Ausdrückliche Erklärung
  - Sonstige eindeutige bestätigende Handlung

Der Widerruf, Art. 7 Abs. 3 DSGVO

- Die betroffene Person hat die Recht, ihre Einwilligung jederzeit zu widerrufen.
- Die Rechtmäßigkeit der Verarbeitung wird bis zum Widerruf nicht berührt.
- Der Widerruf der Einwilligung muss für die betroffene Person mindestens so einfach wie die Erteilung der Einwilligung sein.

Stiftung Tierärztliche Hochschule Hannover
University of Veterinary Medicine Hannover, Foundation

Datenschutz in der Tierarztpraxis

Geht das noch auf eine Kuhhaut?

Wolfgang Rottwinkel
Behördlicher Datenschutzbeauftragter