bpt-info April 2018

Rubrik: Recht

Noch einmal zur EU-Datenschutz-Grundverordnung: Was kommt konkret auf die Tierärztinnen und Tierärzte zu?

„Wir sind alle keine IT-Experten“ – zumindest nicht die meisten von uns, doch diese Erkenntnis nützt uns nicht viel, denn der 25.05.2018 rückt immer näher. An diesem Tag wird die EU-Datenschutz-Grundverordnung (im Folgenden: DSGVO) in Kraft treten, und dies soll Anlass dafür sein, im Anschluss an die bereits im Januar und März an dieser Stelle erschienen Beiträge nachfolgend noch einmal die wichtigsten Punkte aus der Sicht eines Tierarztes, den wir einmal *Dr. DATENLIEB*, nennen, herauszustellen.

Es gilt zu beachten: Der Schutz personenbezogener Daten ist ein besonderes Anliegen des bundesdeutschen Gesetzgebers und auch der Europäischen Kommission, wie es insbesondere mit der im nächsten Monat in Kraft tretenden DSGVO zum Ausdruck kommen wird. Ein jeder Inhaber einer tierärztlichen Praxis, der Leistungen gegenüber einem „Betroffenen“ (also einem Kunden – in diesem Sinne gegenüber einer Privatperson) erbringt bzw. erbringen möchte, wird die Grundsätze der DSGVO beachten müssen.

Rechtliche Grundlagen für die Datenverarbeitung

Wenn Tierarzt Dr. DATENLIEB mit dem Besitzer eines Tieres einen Untersuchungs- oder Behandlungsvertrag abschließen will, geht es um die Anbahnung oder aber Erfüllung eines Vertragsverhältnisses. Er benötigt hierzu die entsprechenden Angaben – wie Name, Anschrift und ggf. Telefonnummer -; darüber hinausgehende Angaben wie E-Mail Adresse, Geburtsdatum, Kontodaten und andere werden allerdings für die Erfüllung eines Vertrages nicht benötigt. Wichtig zu wissen ist, dass es hinsichtlich der Grunddaten zur Begründung und Abwicklung des Vertrages keiner gesonderten Einwilligung des Kunden bedarf, wohl aber für darüber hinausgehende Daten und Zwecke. Ist der Vertrag erfüllt und abgewickelt worden, gibt es grundsätzlich keine Gründe mehr dafür, diese weiter aufzubewahren bzw. zu speichern (abgesehen von berufs- und steuerrechtlichen Gesichtspunkten).

Tierarzt Dr. DATENLIEB hat – z. B. auf den vom Kunden auszufüllenden Patientenaufnahmeschein – auf die jederzeitige Widerrufbarkeit der Einwilligung hinzuweisen. Es sollte dabei nach den Grund- und den freiwilligen Daten getrennt werden. Möglich ist die Einholung einer elektronischen Einwilligung, doch darf hierzu keine voreingestellte Einwilligung in Form eines Häkchens verwendet werden. Darüber hinaus ist der Auftraggeber darüber zu informieren, zu welchem Zweck die Daten verarbeitet werden sollen (also: Erfüllung des Untersuchungs-/Behandlungsvertrages). Es bedarf in diesem Zusammenhang auch einer Überprüfung, ob die bisherigen bereits eingeholten Einwilligungen den Anforderungen der DSGVO entsprechen. Wenn dies nicht der Fall ist, wenn also insbesondere der Hinweis auf den jederzeitigen Widerruf oder die Angabe des

Zwecks fehlen sollte, müssen die Einwilligungen neu eingeholt werden – und dies gilt auch dann, wenn zwar Einwilligungen vorliegen, diese aber (weil ggf. nur mündlich erteilt) nicht nachgewiesen werden können. Die Einwilligungen sind zu dokumentieren.

Informationspflichten

Aufgrund der erweiterten Informationspflichten wird Tierarzt Dr. DATENLIEB nunmehr weitergehende Angaben machen müssen, als es in der Vergangenheit erforderlich war. Zu diesen zählen:

- sein Name und seine Kontaktdaten als Verantwortlicher sowie ggf. seines Vertreters
- Kontaktdaten des – soweit erforderlich – Datenschutzbeauftragten (s. dazu noch weiter unten)
- Zwecke der Verarbeitung und Rechtsgrundlage
- ggf.: sein berechtigtes Interesse
- den Empfänger oder die Kategorie von Empfängern
- Dauer der Datenspeicherung
- Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht und Recht auf Datenübertragbarkeit
- Recht auf Widerruf einer Einwilligung
- Bestehen eines Beschwerderechts gegenüber einer Aufsichtsbehörde
- Absicht der Übermittlung in ein Drittland – dürfte in tierärztlichen Praxen selten vorkommen
- Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling (in tierärztlichen Praxen auch nur von untergeordneter Bedeutung).

Erforderlich ist, diese Informationspflichten zum Zeitpunkt der Erhebung gegenüber dem Kunden zu erfüllen. Falls diese nicht bei der betroffenen Person erhoben wurden, muss die Quelle angegeben werden, aus der die Daten stammen.

Verfügt Tierarzt Dr. DATENLIEB über eine Internetseite (wie es nahezu durchweg gang und gäbe ist)? Dann muss er angeben, ob und welche Cookies verwendet werden und ob sie die Nutzer der Seiten trackt (*nachverfolgt*). Nimmt er hierfür die Dienste einer EDV-Firma/eines Website Gestalters in Anspruch, ist hierüber eine gesonderte Vereinbarung über die Auftragsverarbeitung abzuschließen.

Inanspruchnahme der Dienstleistungen von Dritten

Nimmt Tierarzt Dr. DATENLIEB bei der Datenverarbeitung die Dienste eines anderen Unternehmens in Anspruch, so wäre an folgende Punkte zu denken:

- Es kommt nicht selten vor, dass die Buchführung einer tierärztlichen Praxis – insbesondere mit der Gehaltsabrechnung der Mitarbeiter – über einen Steuerberater abgewickelt wird – dann muss, wenn nicht schon geschehen, ein entsprechender Vertrag mit diesem abgeschlossen werden.

- Zur Geltendmachung und Durchsetzung von Honorarforderungen werden nicht selten tierärztliche Verrechnungsstellen oder Inkassounternehmen eingeschaltet, um säumige Kunden zur Zahlung auffordern zu lassen – hier bedarf es ebenfalls des Abschlusses eines Dienstvertrages. Es bedarf eines ausdrücklichen Hinweises dahingehend, dass die Abrechnung der Honorarforderung und/oder die Durchsetzung ausstehender Zahlungen ein Inkassounternehmen/eine TVS mit der Wahrnehmung der Interessen beauftragt wird.

- Verarbeitet Dr. DATENLIEB die Daten auf einem eigenen Server oder auf dem eines Dritten? Im zuletzt genannten Fall muss eine schriftliche Vereinbarung über eine Auftragsverarbeitung geschlossen werden, denn der IT-Dienstleister darf die Daten nur nach Weisung verarbeiten. Liegen die Daten auf dem eigenen Server, wird aber eine Cloud-Anwendung genutzt, ist zu klären, ob die Daten in Deutschland, in Europa oder in den USA gespeichert werden. Bei einer Übermittlung in die USA handelt es sich um einen Datentransfer in dritte Länder, sodass es hierzu einer besonderen Grundlage bedarf.

- Noch einmal zum Stichwort „Internet“: Wenn dieser von einer Webdesign Agentur gestaltet wird und diese Zugriff auf personenbezogene Daten hat, ist ebenfalls eine Verarbeitung über Auftragsverarbeitung abzuschließen. Auf Grund des hier ebenfalls geltenden Telemediengesetzes ist Dr. DATENLIEB verpflichtet, ein Impressum mit folgenden Angaben zu haben: Name, Anschrift, Rechtsform, E-Mail Adresse, Umsatzsteuer-Identifikationsnummer – wie bereits in unserer Infoschrift: *„Das Wichtigste aus rechtlicher Sicht zur Einrichtung einer tierärztlichen Homepage“* (abrufbar über unseren Bestellservice) näher ausgeführt.

- Wird möglicherweise ein elektronischer Bezahldienst genutzt (z. B. PayPal, Paydirekt, Giropay, usw.), dann ist auch hierüber ein Vertrag abzuschließen.

Mitarbeiter- / Beschäftigten-Datenschutz

Von Bedeutung ist der Datenschutz auch, wenn Assistentinnen und Assistenten, Tiermedizinische Fachangestellte, Auszubildende und sonstige Mitarbeiterinnen und Mitarbeiter in einer tierärztlichen Praxis beschäftigt werden. So dürfen personenbezogene Daten von Beschäftigten verarbeitet werden, sofern dies für die Zwecke der Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses erforderlich ist. Dies sind ohne weiteres Name und Anschrift der Beschäftigten und deren Kontodaten. Weitergehende Informationen bedürfen einer Einwilligung des Betroffenen.

Doch nicht nur der „Verantwortliche“, also TA Dr. DATENLIEB, ist an den Datenschutz gebunden – dies sind auch die Beschäftigten selbst: Diese können dazu verpflichtet werden, über alle Daten Stillschweigen zu bewahren, von denen sie im Rahmen ihrer Beschäftigung Kenntnis erlangen („Verpflichtung auf Vertraulichkeit“).

Datenschutz und Videoüberwachung: zulässig?

Eine Videoüberwachung von Mitarbeitern/Arbeitnehmern ist derzeit „offen“ möglich, wenn die Voraussetzungen nach § 6b des Bundesdatenschutzgesetzes eingehalten

werden, insbesondere, wenn die betroffenen Personen hierüber informiert werden. Auch eine verdeckte Videoüberwachung ist gestattet, allerdings nur dann, wenn ein konkreter Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers vorliegt, weniger einschneidende Mittel ausgeschöpft sind und die Videoüberwachung als einziges Mittel verbleibt und insgesamt nicht unverhältnismäßig ist. Sozialräume dürfen dabei grundsätzlich nicht überwacht werden. Die DSGVO enthält allerdings keine konkrete Regelung zur Zulässigkeit zur Videoüberwachung, auch wenn möglicherweise davon auszugehen ist, dass künftig geringere datenschutzrechtliche Anforderungen an die Zulässigkeit einer Videoüberwachung gestellt werden. Im Übrigen ist dieses Thema allerdings so komplex, dass wir auf dieses noch einmal zu einem späteren Zeitpunkt zurückkommen werden.

Datenschutz und „Datenschutzmanagement“

Im Verhältnis zur bislang geltenden Rechtslage neu ist die Verpflichtung von TA Dr. DATENLIEB, seine Verfahren in einem „Verzeichnis über Verarbeitungstätigkeiten“ mit folgenden Angaben zu dokumentieren:

- seinen Namen und seine Kontaktdaten (ggf. des Stellvertreters, und soweit vorhanden des Datenschutzbeauftragten)
- Zweck der Verarbeitung
- Rechtsgrundlage
- Kategorie der betroffenen Personen und personenbezogene Daten
- Kategorie von Empfängern der Daten
- Übermittlung in Drittstaaten (wohl nur selten)
- Löschfristen und
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Datensicherung.

Von besonderer Bedeutung in diesem Zusammenhang sind Auskunfts- und Löschungsverlangen der Betroffenen: Es sollte ein Verfahren für den Fall festgelegt werden, dass jemand erfahren möchte, welche Daten über ihn gespeichert worden sind. Und es muss auch ein Löschkonzept vorgehalten werden, in dessen Rahmen zu beachten ist, dass berufsrechtliche Aufzeichnungen in der Regel für 5 steuerrelevante Unterlagen sogar für 10 Jahre aufzubewahren sind. Andere Daten sind – auch ohne Aufforderung des Betroffenen – zu vernichten, wenn sie nicht mehr benötigt werden. Dies kann in der Form geschehen, dass Datensätze gelöscht, Datenträger zerstört oder Papierunterlagen mit personenbezogenen Daten geschreddert werden.

Was muss Tierarzt Dr. DATENLIEB bei Datenverstößen veranlassen?

Der Schutz personenbezogener Daten kann auch verletzt werden – in dem Daten z. B. unberechtigt an Dritte herausgegeben werden. Derartige Verletzungen müssen unverzüglich, nach Möglichkeit innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls, an die zuständige Aufsichtsbehörde gemeldet werden. Die Benachrichtigung muss eine Beschreibung der Art der Verletzung, Kategorien und Zahl der betroffenen Personen und Datensätze, den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle sowie eine Beschreibung der wahrscheinlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen

zur Behebung oder Abmilderung der Verletzung enthalten. Auch der Betroffene hat eine Benachrichtigung zu erhalten, wobei aber zahlreiche Ausnahmen bestehen (so z. B., wenn im Vorfeld geeignete IT-Sicherheitsmaßnahmen wie z. B. durch Verschlüsselung getroffen oder nach einer Datenpanne geeignete IT-Sicherheitsmaßnahmen getroffen worden sind). Kommt es bei einem Auftragsdatenverarbeiter (s. oben „Inanspruchnahme der Dienstleistungen von Dritten“) zu einem Datenschutzverstoß, muss dieser seinen Auftraggeber, also Herrn Dr. DATENLIEB als verantwortlichen Praxisinhaber, informieren.

Technisch-organisatorische Maßnahmen

Die am 25.05.2018 in Kraft tretende DSGVO zwingt alle Unternehmen und damit auch Herrn Dr. DATENLIEB dazu, technische und organisatorische Maßnahmen zu treffen, um nicht nur den Schutz, sondern auch die Sicherheit der zu verarbeitenden personenbezogenen Daten ihrer Kunden und Mitarbeiter zu gewährleisten. Dies bedeutet zwar keine grundlegende Neuerung gegenüber dem bisherigen Bundesdatenschutzgesetz, doch angesichts der hohen möglichen Sanktionen ist auch Herr Dr. DATENLIEB gut beraten, die erforderlichen Maßnahmen in der eigenen Praxis rechtzeitig zu überprüfen. Die DSGVO zählt einige wenige aber sehr wirksame Schutzmaßnahmen auf, die dem Grunde nach selbstverständlich sein sollten. In Artikel 32 DSGVO werden folgende technisch-organisatorische Maßnahmen genannt:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wieder herzustellen und
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Mit anderen Worten: Es geht um Maßnahmen, die wirksam sicherlich nur mit Hilfe der IT-Firma umgesetzt werden können!

Bestellung eines betrieblichen Datenschutzbeauftragten

Schon nach der bisherigen Rechtslage (Bundesdatenschutzgesetz) könnte Tierarzt Dr. DATENLIEB verpflichtet gewesen sein, einen betrieblichen Datenschutzbeauftragten zu benennen. Unter welchen Voraussetzungen aber ist dies erforderlich, wenn ab 25.05.2018 die DSGVO in Kraft tritt? Die Antwort hierauf lautet: Der betriebliche Datenschutzbeauftragte ist zwingend zu bestellen, wenn die Kerntätigkeit des Verantwortlichen in Verarbeitungsvorgängen besteht, welche aufgrund Art, Umfang und/oder Zweck eine umfangreiche regelmäßige und systematische Beobachtung personenbezogener Daten erforderlich machen. Unter „Kerntätigkeit“ fallen hierbei Geschäftsbereiche, die für die Umsetzung der Unternehmensstrategie erforderlich sind (Stichwort: „Kundenservice“). Das inzwischen neu gefasste Bundesdatenschutzgesetz behält die bisherige Regelung

weitgehend bei, d. h. ein Datenschutzbeauftragter ist zu bestellen, wenn mindestens 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind – wozu bereits das Schreiben und die Empfangnahme/das Lesen von E-Mails gehört. Wichtig zu wissen ist: Nicht bestellt darf eine Person, die in einen Interessenkonflikt geraten könnte oder für die eine Gefahr der Selbstkontrolle besteht – Dr. DATENLIEB ist somit von einer Bestellung ausgeschlossen, ebenso wie es bei einem Partner/einer Partnerin (falls Dr. DATENLIEB eine Gemeinschaftspraxis führen sollte) der Fall wäre.

Was hat es mit der Datenschutzfolgenabschätzung zu tun

..... wird sich nicht nur Tierarzt Dr. DATENLIEB fragen. In aller Kürze zusammengefasst: Eine solche ist notwendig, wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, z. B. bei Verwendung neuer Techniken oder aber wenn sie aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung erforderlich ist.

Die Datenschutzfolgenabschätzung erfolgt in drei Stufen:

- In der ersten Stufe ist zu prüfen, ob ein hohes Risiko für Rechte und Freiheiten der Betroffenen besteht. Hauptanwendungsgebiete sind Technologien, die automatisiert, systematisch und umfassend Daten erfassen, verarbeiten und bewerten – doch ggf. auch nur vereinzelte Daten, wenn aus diesen z. B. hervorgeht, dass das behandelte Tier an einer Erkrankung leidet, die auf seinen Halter/Eigentümer (Auftraggeber der tierärztlichen Leistung) übertragbar ist.

- Besteht ein solches Risiko, ist in einer nachfolgenden Stufe eine Bewertung dahingehend vorzunehmen, ob die geplanten Abhilfemaßnahmen und Sicherheitsvorkehrungen ausreichend sind, um den Schutz der Daten zu gewährleisten. Außerdem ist der Nachweis zu bringen, dass die DSGVO eingehalten und den Interessen der Betroffenen Rechnung getragen wird.

- Kommt die Bewertung zu dem Ergebnis, dass trotz möglicher Maßnahmen ein hohes Risiko besteht, muss in einer dritten Stufe die Aufsichtsbehörde konsultiert werden; diese kann sodann innerhalb von 8 Wochen Empfehlungen aussprechen.

Ist in dem Unternehmen ein betrieblicher Datenschutzbeauftragter bestellt worden (s. oben), so muss er mit in die Datenschutzfolgenabschätzung eingebunden werden. Die Folgenabschätzung ist schriftlich zu dokumentieren, wobei es zweckmäßig sein kann, diese mit dem Verzeichnis der Verarbeitungstätigkeiten zu verknüpfen.

Verzeichnis der Verarbeitungstätigkeiten

Einer der Kernpunkte der DSGVO ist die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten. Was bedeutet dies, wird sich sicherlich nicht nur Tierarzt Dr. DATENLIEB fragen. Worum geht es also? Nach der DSGVO muss ein jedes Unternehmen eine Übersicht darüber führen, welche personenbezogenen Daten es aus welchen Gründen und wie lange bearbeitet. Das Verzeichnis von TA Dr.

DATENLIEB muss daher folgende Angaben in schriftlicher oder elektronischer Form beinhalten:

- seinen Name und seine Kontaktdaten und des Datenschutzbeauftragten (wenn erforderlich)
- Zwecke der Datenverarbeitung
- betroffene Personen und betroffene Daten
- Empfänger von Daten, falls sie weitergegeben werden
- Übermittlungen in Drittländer, ggf. Rechtsgrundlage (allenfalls im „kleinen Grenzverkehr“) denkbar
- Löschungsfristen pro Datenkategorie, wenn möglich
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen wenn möglich (s. oben)

Auch Auftragsverarbeiter müssen eine Dokumentation führen, denn sie gelten zukünftig – und dies wird gegenüber der bisherigen Rechtslage neu sein – als ebenso verantwortlich für den Datenumgang wie der Auftraggeber (Verantwortlicher – Praxisinhaber) selbst. Es ist festzuhalten:

- Name und Kontaktdaten von Auftraggeber, Auftragnehmer und des etwaigen Datenschutzbeauftragten
- Kategorien von Verarbeitungen, die im Auftrag durchgeführt werden
- Übermittlungen in Drittländer plus Rechtsgrundlage und
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, wenn möglich.

Verantwortlich für die Dokumentation ist in erster Linie das Unternehmen (der Praxisinhaber), nicht der Datenschutzbeauftragte. Aufgabe des letzteren besteht darin, die Einhaltung der Datenschutzvorschriften zu überwachen – und damit eben auch, ob das „Verzeichnis der Verarbeitungstätigkeiten“ geführt wird.

Recht des Betroffenen auf Löschung („Recht auf Vergessenwerden“)

Darf denn Tierarzt Dr. DATENLIEB die Daten seiner Kunden „auf Ewigkeit“ speichern? Nein, denn die Betroffenen haben ein Recht auf Löschung ihrer Daten, wenn

- die Speicherung der Daten nicht mehr notwendig ist
- der Betroffene seine Einwilligung zur Datenverarbeitung widerrufen hat
- die Daten unrechtmäßig verarbeitet wurden
- eine Rechtspflicht zum Löschen nach EU- oder nationalem Recht besteht.

Unberechtigt wäre demgegenüber eine Förderung nach Löschung der Daten, wenn

- die Datenspeicherung der Erfüllung einer rechtlichen Verpflichtung dient (man denke insbesondere an berufs- und steuerrechtliche Vorschriften, wie bereits oben erwähnt)
- die freie Meinungsäußerung bzw. die Informationsfreiheit überwiegen (wohl weniger von Bedeutung) und (wohl kaum von Bedeutung in tierärztlichen Praxen) - das öffentliche Interesse im Bereich der öffentlichen Gesundheit überwiegt
- Archivzwecke, wissenschaftliche und historische Forschungszwecke dem entgegenstehen oder

- die Speicherung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Darüber hinaus können Betroffene verlangen, dass unrichtige personenbezogene Daten berichtigt oder unvollständige vervollständigt werden.

Zusammenfassung und Hinweis

Die neue DSGVO wird es erforderlich machen, bestehende Formulare zu ändern, neue Formulare oder auch Muster-Erklärungen zu erstellen und auch neue Verträge abzuschließen. Einschlägige Muster können zwar zu allen der vorstehend näher beschriebenen DSGVO-Themenbereiche über das Internet abgerufen werden; ab etwa Mitte des Monats werden diese aber zu einem großen Teil aber auch auf der bpt-Homepage (Bestellservice) zur Verfügung stehen.

Michael Panek (bpt.panek@tieraerzteverband.de)