

Checkliste Datenschutz-Grundverordnung

Wir haben für Sie die wichtigsten Aufgaben zur Datenschutz-Grundverordnung, die am 25. Mai 2018 in Kraft tritt, in einer Checkliste gemäß Aufgabenstellung der Datenschutzkonferenz der Länder, der Bayerischen und Bremer Aufsichtsbehörde zusammengestellt.

Aufgabe gemäß Datenschutzkonferenz, LfDI HB und BayLfD	Lösungen für Apothekeninhaber/innen	✓
<p>Chef-Sache, Datenschutzbeauftragter, Mitarbeitersensibilisierung</p> <ul style="list-style-type: none"> Gibt es das Bewusstsein im Unternehmen, dass Datenschutz Chefsache ist? Verfügt Ihr Unternehmen über einen betrieblichen Datenschutzbeauftragten? Sensibilisierung: Mitarbeiter über die Inhalte der DSGVO in Kenntnis setzen. 	<ul style="list-style-type: none"> Ruhe bewahren! Effektiv hat sich im Verhältnis zum (alten) BDSG nicht viel verändert. Wer bisher gesetzeskonform aufgestellt war, hat nichts zu befürchten. Sich bewusst machen, dass ich mich der Aufgabe stellen muss. Inhaltliche Auseinandersetzung mit dem Thema Datenschutz und das ich verantwortliche Stelle bin. (Externen) Datenschutzbeauftragten bestellen, wenn noch nicht geschehen. (Pflicht zur Bestellung ist umstritten. Wir können Ihnen jedoch dazu raten, Siehe Anlage 2 mit Anhang). Mitarbeiter für das Thema Datenschutz schulen und sensibilisieren, wenn noch nicht geschehen. 	<p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p>
<p>Verfahrensverzeichnis: künftig Verarbeitungsverzeichnis</p> <ul style="list-style-type: none"> Sind alle Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen (Artikel 30 DSGVO)? 	<ul style="list-style-type: none"> Erstellung bzw. Aktualisierung eines Verfahrensverzeichnisses (Verarbeitungsverzeichnis neu, Anlage 3) nach den Vorgaben der DSGVO. Dokumentationen der technischen und organisatorischen Maßnahmen, Anlage 4: Wie eine Beschreibung der technisch organisatorischen Maßnahmen (TOM) praktisch aussehen kann, ergibt sich aus den TOM der Anlage 1, Seite 4 und 5) 	<p>_____</p> <p>_____</p>
<p>Zulässigkeit der Verarbeitung</p> <ul style="list-style-type: none"> Sie benötigen für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage. Dies kann eine gesetzliche Regelung oder eine Einwilligung der Betroffenen sein. Sofern Verarbeitung auf Einwilligung beruht: das Recht zum jederzeitigen Widerruf der Einwilligung 	<ul style="list-style-type: none"> Für die Rezeptabrechnung im GKV-Bereich über das Apothekenrechenzentrum gelten die gesetzlichen Rechtsgrundlagen gemäß §§ 300 und 302 SGB V sowie § 105 SGB XI. Hier ist nichts zu unternehmen. Für die Privatrezep tabrechnung muss eine Einwilligungserklärung des Patienten vorliegen (Anlage 5) Bei der Verarbeitung und Speicherung der Patientendaten zur Erstellung von Zuzahlungsquittungen müssen Einwilligungserklärungen der Patienten vorliegen (Anlage 5). Für die Verarbeitung sonstiger Kundendaten, z.B. im Rahmen des Einsatzes von Kundenkartensystemen o.ä. muss eine Einwilligungserklärung des Patienten vorliegen (Anlage 5). 	<p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p>

Aufgabe gemäß Datenschutzkonferenz, LfDI HB und BayLfD	Lösungen für Apothekeninhaber/innen	✓
<p>Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen</p> <ul style="list-style-type: none"> Für jeden Datenverarbeitungsprozess überprüfen, ob Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen einzurichten ist. 	<ul style="list-style-type: none"> Mit dem (externen) IT-Berater, bzw. IT-Administrator, dem Warenwirtschaftssystemanbieter und dem Apothekenrechenzentrum sprechen, welche Möglichkeiten im Zusammenhang mit dem jeweiligen System bestehen, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen einzurichten. Die Ergebnisse der Gespräche sollten dokumentiert werden. 	<hr/> <hr/>
<p>Auftragsdatenverarbeitungsverträge</p> <ul style="list-style-type: none"> Haben Sie Ihre bestehenden Verträge mit externen Auftragsdatenverarbeitern, das heißt mit Unternehmen, die in Ihrem Auftrag personenbezogene Daten verarbeiten, an die neuen Regelungen (Artikel 26 – 28 DSGVO) angepasst? Dokumentieren Sie Anweisungen, die Sie Ihren Auftragsdatenverarbeitern geben? 	<ul style="list-style-type: none"> Das Apothekenrechenzentrum (NARZ/AVN: Anlage 1), der Warenwirtschaftsanbieter und mein Apothekerverein/-verband (für Hilfsmittelclearing und Retaxbearbeitung) übersenden mir eine nach der DSGVO angepassten Vereinbarung zur Datenverarbeitung im Auftrag. Diese Vereinbarung schließe ich ab. Sonstige Dritte, die für mich personenbezogene Daten im Auftrag verarbeiten bitte ich um Übersendung einer nach der DSGVO angepassten Vereinbarung zur Datenverarbeitung im Auftrag und schließe diese ab. 	<hr/> <hr/>
<p>Datenschutz-Folgenabschätzung</p> <ul style="list-style-type: none"> Führt Ihr Unternehmen Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen durch (Artikel 35 DSGVO)? Dies gilt zum Beispiel bei einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten (=Gesundheitsdaten). Falls ja, haben Sie für die in diesen Fällen erforderliche Datenschutz-Folgenabschätzung in Ihrem Unternehmen einen Prozess eingeführt? Wer ist für diesen Prozess zuständig? 	<ul style="list-style-type: none"> Eine Datenschutzfolgeabschätzung ist bei der Verarbeitung von Gesundheitsdaten immer erforderlich. <ol style="list-style-type: none"> Verarbeite ich mit dem (Arbeits-) Prozess Personenbezogene Gesundheitsdaten und Daten Minderjähriger (oder Gesundheitsdaten in einem größeren Umfang)? Wenn ja, Einschätzung der Eigenart der betreffenden Verarbeitung, des Umfangs, Kontext und Zweck Einschätzung der Risiken, insbesondere der Eintrittswahrscheinlichkeit und Schwere der möglichen Verletzung von Rechten (vgl. hierzu Anlage 6 vom Bayerischen Landesamtes für Datenschutzaufsicht) Risikominimierung, Sicherstellung der Einhaltung der DSGVO, Dokumentation Für den Prozess der Datenschutzfolgeabschätzung bin ich zuständig. Der (externe) betriebliche Datenschutzbeauftragte - soweit bestellt - unterstützt mich hierbei beratend und kann mir viele Tätigkeiten abnehmen. 	<hr/> <hr/>

Checkliste Datenschutz- Grundverordnung

Aufgabe gemäß Datenschutzkonferenz, LfDI HB und BayLfD	Lösungen für Apothekeninhaber/innen	✓
<p>Meldepflichten</p> <ul style="list-style-type: none"> • Haben Sie in Ihrem Unternehmen einen Prozess zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde eingeführt (Artikel 33 DS-GVO)? • Haben Sie dabei insbesondere auch die Einhaltung der Meldefrist von 72-Stunden beachtet? • Wer ist in Ihrem Unternehmen für die Meldung zuständig? • Meldung der Kontaktdaten des Datenschutzbeauftragten an die Aufsichtsbehörde. 	<ul style="list-style-type: none"> • Der (externe) betriebliche Datenschutzbeauftragte definiert und dokumentiert einen Prozess zur Meldung von Datenschutzverstößen an die zuständige Datenschutzaufsichtsbehörde. • Hierbei wird die 72-Stundenfrist mit berücksichtigt. • Der (externe) betriebliche Datenschutzbeauftragte ist für die Meldung zuständig und meldet auch seine Kontaktdaten an die Aufsichtsbehörde. 	<p>_____</p> <p>_____</p> <p>_____</p>
<p>Betroffenenrechte und Informationspflichten</p> <ul style="list-style-type: none"> • Die Betroffenen sind über die Verarbeitung ihrer Daten zu informieren. Dies hat insbesondere in einer transparenten, leicht zugänglichen Form sowie in einer klaren und einfachen Sprache zu erfolgen (Artikel 12 DS-GVO). • Haben Sie Ihre Texte zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 bzw. 14 DS-GVO angepasst? • Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Auskunft zu den eigenen Daten nach Art. 15 DS-GVO zeitnah und vollständig erfüllen zu können • Bestehen der Rechte betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Widerspruch aufgrund besonderer Situation einer betroffenen Person sowie auf Datenportabilität (Datenübertragung vom Verantwortlichen an Einwilligenden). 	<ul style="list-style-type: none"> • Die Inhalte zu den Informationspflichten und Betroffenenrechten sollen gemäß Anlage 7 auf der Internetseite, per Aushang in der Apotheke und mittels Flyer am HV den Patienten zugänglich gemacht werden. • Der (externe) betriebliche Datenschutzbeauftragte konzipiert einen Prozess, um Anträge betroffener Personen auf Auskunft zu den eigenen Daten zeitnah und vollständig erfüllen zu können. 	<p>_____</p> <p>_____</p>