VERBAND DEUTSCHER ZAHNTECHNIKER INNUNGEN

VDZI

Einstieg in den Datenschutz – ein Leitfaden

EU-Datenschutz-Grundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG)

Pflichten als Chance für das betriebliche Datenschutzmanagement in einer digitalen Zukunft

Stand: April 2018

EINLEITUNG

Die ganze Welt ist (wird) digital. Privat und geschäftlich nutzen wir den PC, das Notebook, das iPad, das Mobiltelefon. Per LAN oder WLAN vernetzen wir die Geräte und fügen noch den FAX-Drucker, den Bewegungsmelder und die Kamera hinzu. Mit dem Internet eröffnet sich die Vernetzung mit der Außenwelt. Wir laden und senden Daten in die Cloud-Welt, schicken den Kunden Daten per Email, verschlüsselt oder auch nicht, tauschen Daten mit Kollegen auf allen Kanälen aus und präsentieren das Unternehmen auf eigenen Homepages und in allen sozialen Medien.

Wir nutzen die Chancen und Möglichkeiten der Informationswelt, in der wir Wissen sammeln und teilen, multimedial kommunizieren und per Knopfdruck weltweit auf alle Daten zugreifen.
Doch die Möglichkeiten bergen auch Risiken: Immer mehr gespeicherte Daten in der Hand des Staates oder von Unternehmen können zum „gläsernen Menschen“ oder zum „gläsernen Kunden“ führen. Der Datenklau in Unternehmen ist ein weltweites Geschäft. Manipulationen, Rufschädigungen, Erpressungen und andere Erscheinungen des Datenmissbrauchs sind objektive Gefahren für den Einzelnen, aber auch für Unternehmen.

Gesetze und Verordnungen sollen dazu anhalten, diese Gefahren ernst zu nehmen und sie sollen zu mehr Transparenz und Kontrollierbarkeit bei der Verarbeitung personenbezogener Daten führen. Das Ziel ist klar: Ein besserer Schutz der persönlichen Daten. Darum geht es auch in der aktuellen EU-Datenschutz-Grundverordnung (EU-DSGVO), die für einen europaweit einheitlichen Datenschutz sorgen soll.

Die EU-DSGVO ist ab dem 25. Mai 2018 anzuwenden. Vor allem die damit im Zusammenhang gebrachten/stehenden hohen Geldbußen haben die bisherigen Schlagzeilen hierzu dominiert. Viele Anbieter versprechen – zumindest dann, nun das Seelenheil beim Thema Datenschutz, wenn man sie denn nur machen ließe und am Ende die horrende Rechnung für Beratungsleistungen und Neuanschaffungen bezahlt.

Die europäische Verordnung ist in weiten Teilen ein Nachvollzug des deutschen Bundesdatenschutzgesetzes (BDSG). Schon darin war bisher die Einhaltung des strengen Datenschutzes ebenso Pflicht wie beispielsweise das sogenannte Verarbeitungsverzeichnis.

Neu ist aber, dass nun das Unternehmen die Nachweispflicht der Einhaltung einer rechtskonformen Datenverarbeitung trifft. Da man nur nachweisen kann, was man auch dokumentiert, kommt den Dokumentationspflichten in Streit- und Schadensfällen besondere Bedeutung zu.

Die Pflicht beim Einhalten der EU-DSGVO ist für den Unternehmer aber auch eine hervorragende Gelegenheit, seine Kunden- und Datenverwaltung, im Zuge einer immer stärkeren Digitalisierung betrieblicher Prozesse, auf eine zukunftssichere Grundlage zu stellen. Insofern wird aus der Pflicht eine gute Chance und der Datenschutz zu einer Managementaufgabe.

Bitte beachten Sie, dass diese Schrift nur allgemein informieren kann. Jeder Betrieb ist in seiner programmtechnischen Ausstattung und in seiner Arbeitsorganisation sehr individuell. Auch kann hier nicht auf alle weiteren für Datenschutz und Datensicherheit relevanten Gesetze und Regularien eingegangen werden. Bei konkreten Fragen ist die Inanspruchnahme eines Datenschutzbeauftragten, eines IT-Systemhauses oder auch eines Fachanwaltes unverzichtbar.

Ihr VDZI

Ihre Notizen:

Inhalt

Die EU-DSGVO – Was sie regelt

Die Datenschutzgrundverordnung (DSGVO) der Europäischen Union (EU) hat zum Ziel, innerhalb der EU-Staaten ein gleich hohes Datenschutzniveau zu schaffen.

Es werden damit die Grundrechte und Grundfreiheiten natürlicher Personen geschützt, insbesondere deren Recht auf Schutz personenbezogener Daten. Gleichzeitig soll mit den Vorgaben eine stärkere Kontrolle und eine höhere Transparenz bei der Verarbeitung personenbezogener Daten erreicht werden. Die DSGVO ist ab dem 25. Mai 2018 anzuwenden. Gleichzeitig mit der DSGVO tritt das BDSG neu in Kraft. Dieses Gesetz regelt den Datenschutz allerdings nur soweit wie die DSGVO vorsieht, dass bestimmte Datenschutzbereiche auf nationaler Ebene geregelt werden dürfen oder müssen.

Insofern ist bei der konkreten Umsetzung des Datenschutzes immer beides zu beachten, die EU-DSGVO, soweit sie unmittelbar gilt, und die Vorschriften des BDSG-neu.

Was sind personenbezogene Daten?

Gemäß der EU-DSGVO sind personenbezogene Daten alle Informationen, die zur Identifizierbarkeit einer natürlichen Person beitragen. Dazu gehören beispielsweise die Namen von Personen, die privaten und geschäftlichen Kontaktdaten (u. a. Anschriften, E-Mail-Adressen, Festnetz- oder Mobilnummern) ebenso wie Bilder, aber auch Standortdaten, Bankdaten, Geburtstage, Hobbys sind nicht zu vergessen. Besonderes Augenmerk erfordern Daten der Internetwelt wie Nutzernamen, Profilbilder, IP-Adressen und sogenannte Cookie-IDs sowie Beiträge in den Social Media-Kanälen – dies alles ohne Unterscheidung zwischen personenbezogenen Daten im privaten, öffentlichen oder arbeitsbezogenen Umfeld einer Person, denn Geschäftsbeziehungen werden immer von einzelnen (natürlichen) Personen gepflegt.

Welche Vorgänge der Datenverarbeitung sind betroffen?

Generell beinhaltet der Datenschutz alle Vorgänge mit personenbezogenen Daten. Die EU-Verordnung fasst dies unter „Verarbeitung" zusammen, darunter versteht man:

- jeden ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten die
- mit oder ohne* der Hilfe automatisierter Verfahren erfolgen.

* auch diese „analogen" Dokumente enthalten personenbezogene Daten:

Auftragszettel aus der Zahnarztpraxis
Eingehendes Fax mit personenbezogenen Daten
Druckergebnisse am frei zugänglichen Drucker
Kunden- und Auftragsakten in den Regalen im Büro
Rechnungsordner Ihrer Lieferanten und Kunden
Personalakten, Lohnbuchhaltungsdaten, Urlaubskarteien

Betroffene Vorgänge:

- das Erheben oder Erfassen,
- die Organisation oder das Ordnen,
- die Speicherung,
- die Anpassung oder Veränderung,
- das Auslesen, Abfragen oder 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.

Was setzt die Verarbeitung personenbezogener Daten voraus?

Allgemeiner Grundsatz für die Verarbeitung personenbezogener Daten ist ein sogenanntes Verbot mit Erlaubnisvorbehalt. Die Verarbeitung von personenbezogenen Daten ist demnach grundsätzlich nur dann zulässig, wenn eine Einwilligung der betroffenen Person, bspw. des Kundens, (oder eine gültige Ausnahme nach Art. 6 EU-DSGVO) vorliegt.

Grundsätzlich besteht eine Informationspflicht über die Verarbeitung von personenbezogenen Daten. Sie sind dazu angehalten, Betroffene vorab darüber zu informieren, wenn Sie personenbezogene Daten verarbeiten:

Ein Muster zur Information bei der Erhebung von personenbezogenen Daten an Betroffene entnehmen Sie bitte der Anlage 1.

Der Erlaubnisvorbehalt

Grundsätzlich besteht eine Informationspflicht über die Verarbeitung von personenbezogenen Daten. Sie sind dazu angehalten Betroffene vorab darüber zu informieren, wenn Sie personenbezogene Daten verarbeiten. Eine rechtmäßige Einwilligung liegt vor, wenn folgende Bedingungen erfüllt sind.

Nachweispflicht

Der Verantwortliche muss nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten für einen oder mehrere bestimmte Zwecke eingewilligt hat.

Klare Trennung

Erfolgt die schriftliche Einwilligung im Zusammenhang mit anderen Sachverhalten, so muss das Ersuchen um Einwilligung zur Datenverarbeitung so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Außerdem muss das Ersuchen in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen.

Hinweis auf Widerrufsrecht

Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

Freiwilligkeit

Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden.

Zweck- und Verarbeitungsbezug

Die betroffene Person ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

Ohne Einwilligung gemäß Art. 6 EU-DSGVO

Gemäß Art. 6 EU-DSGVO ist eine Datenverarbeitung ohne Einwilligung zulässig:

- zur Erfüllung eines Vertrags (z. B. Adresse des Kunden, um den Auftrag vor Ort beim Kunden ausführen zu können).
- zur Durchführung vorvertraglicher Maßnahmen (z. B. E-Mail-Adresse, um dem Kunden wunschgemäß einen Kostenvoranschlag senden zu können)
- zur Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses (z. B. Speicherung von Lohnunterlagen und Krankheitstagen)
- zur Ausübung der Interessensvertretung der Beschäftigten (z. B. Weiterleitung von Arbeitnehmerdaten an den Betriebsrat)

Ohne Einwilligung gemäß Art. 9 EU-DSGVO

Für Betriebe der Gesundheitshandwerke folgt die Berechtigung zur Verarbeitung von Patientendaten ohne Einwilligung als Gesundheitsdaten aus Art. 9 EU-DSGVO. Diese Vorschrift erlaubt die Verarbeitung von Gesundheitsdaten:

- zum Zweck der Gesundheitsvorsorge
- zur Versorgung oder Behandlung im Gesundheits- oder Sozialbereich
- wenn es für einen Vertrag zwischen der betroffenen Person und einem Angehörigen eines Gesundheitsberufs erforderlich ist

Was für die Zahntechniker gilt:

Verarbeitet das zahntechnische gewerbliche Labor personenbezogene Daten in der Art und dem Umfang, wie sie zur Erfüllung der vertraglichen Pflichten zur Auftragserfüllung gegenüber dem Zahnarzt erforderlich sind, so bedarf es aus diesem Grund keiner gesonderten Einwilligung. Da zudem weite Teile der erforderlichen Daten als Gesundheitsdaten nach Art. 9 EU-DSGVO anzusehen sind, bedarf es auch aus diesem Grund keiner Einwilligung.

Hinweis:
Für alle anderen Prozesse bei der Verarbeitung von personenbezogener Daten welche nicht durch Art. 6 und Art. 9 EU-DSGVO geregelt sind, ist eine Einwilligung der Betroffenen erforderlich!

Was die betroffene Person von Ihnen verlangen darf

Mit der EU-DSGVO erhalten Einzelpersonen mehr Kontrolle über ihre Daten (Betroffenenrechte). Dazu gehören u. a.:

Informationsrecht

Die betroffene Person muss vor dem Erheben und der Erfassung ihrer personenbezogenen Daten informiert werden. Sie muss explizit in die Erfassung der Daten einwilligen.

Recht auf Auskunft

Die betroffene Person hat das Recht, eine Auskunft darüber zu erhalten, ob und welche ihrer Daten verarbeitet werden sowie weitere Auskunft/Informationen u. a. zu Verarbeitungszweck, Herkunft und Empfänger der Daten, Dauer der Speicherung und ihren Rechten.

Recht auf Berichtigung

Die betroffene Person kann verlangen, dass falsch oder unvollständig gespeicherte Daten berichtigt oder vervollständigt werden.

Recht auf Löschung („Recht auf Vergessenwerden“)

Die betroffene Person kann die unverzügliche Löschung ihrer Daten verlangen, wenn bspw. der ursprüngliche Zweck ihrer Verarbeitung nicht mehr besteht, die erteilte Einwilligung widerrufen wird, Widerspruch gegen die Verarbeitung eingelegt wird oder Daten unrechtmäßig verarbeitet wurden. In der EU-DSGVO aufgeführte Ausnahmen sind zu beachten.

Recht auf Einschränkung der Verarbeitung

Die betroffene Person kann die Einschränkung der Verarbeitung von Daten verlangen, wenn diese bspw. nicht korrekt sind, unrechtmäßig verwendet werden, die Einwilligung zur Verarbeitung der Daten widerrufen wurde oder die Löschung aus anderen Gründen unzulässig ist.

Recht auf Datenübertragbarkeit

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, welche sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und sie hat das Recht, diese Daten an einen anderen Verantwortlichen zu übermitteln oder übermitteln zu lassen.

Widerspruchsrecht

Die betroffene Person kann bezogen auf unterschiedliche Verwendungszwecke der Verarbeitung ihrer Daten jederzeit widersprechen. Bei der ersten Kommunikation muss auf das Widerspruchsrecht in einer verständlichen und von anderen Informationen getrennten Form hingewiesen werden.

Die vorgenannte Auszählung zeigt, die Rechte der Personen werden in der EU-DSGVO ausdrücklich gestärkt. Ein Kunde, ein Lieferant oder ein Mitarbeiter hat z. B. das Recht auf Berichtigung, Sperrung und Löschung seiner Daten. Außerdem hat er das Recht, unentgeltlich Informationen über alle gespeicherten personenbezogenen Daten zu erhalten – nach dem Recht auf Datenübertragbarkeit auch in einem strukturierten, gängigen und maschinenlesbaren Format.

Unser Tipp:

Was ist bei Anfragen zu beachten?

Vor der Auskunftserteilung ist die Identität des Anfragenden zu prüfen!

- Es besteht ein Auskunftsrecht für Betroffene.
- Alle Betroffenenanfragen sind möglichst präzise und einfach verständlich zu beantworten.
- Im Idealfall sollte eine Antwort schriftlich erfolgen.
- Auskunftsersuchen sind innerhalb von 4 Wochen zu bearbeiten.
- Auskunftserteilung sollte für den Betroffenen kostenlos möglich sein.

Für die Beantwortung von Auskunftsersuchen von Betroffenen entnehmen Sie das Musterformular aus der Anlage 2.

Prüfen Sie Ihre EDV-Programme

Um dem Recht auf Auskunft einer Person lückenlos und ohne großen Aufwand nachkommen zu können, sollten Sie prüfen, ob Ihre Programme

- die Erfassung, Bearbeitung, Änderungen und Verwendungen personenenbezogener Daten, etwa mittels Journalfunktion, dokumentieren.
- dokumentieren, welche Daten an wen weitergegeben wurden und ob hierfür die nötige Erlaubnis vorlag.
- über Reportfunktionen Ausdrucke erzeugen, die alle zur Personen gespeicherte Daten auflisten.
- über Export-Funktionen in verschiedene Dateiformate verfügen, um so dem Recht auf Datenübertragbarkeit nachkommen zu können.

Wie Sie mit personenbezogenen Daten umgehen müssen

Die EU-DSGVO schreibt die bisherigen datenschutzrechtlichen Grundsätze fort und entwickelt sie weiter:

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben sowie in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

Zweckbindung

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Ändert sich der ursprüngliche Zweck, muss dies kommuniziert werden.

Datensparsamkeit/-minimierung

Weniger ist mehr: Es dürfen nur die personenbezogenen Daten in einem notwendigen Maß erhoben und verarbeitet werden, die für einen bestimmten Zweck angemessen und relevant sind.

Richtigkeit

Personenbezogene Daten müssen sachlich richtig und wenn nötig auf dem neuesten Stand sein. Es sind alle Maßnahmen zu ergreifen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Speicherbegrenzung

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Danach sind die personenbezogenen Daten zu löschen oder zu anonymisieren. Ausnahmen der EU-DSGVO hierzu sind zu beachten.

Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Einhaltung der Grundsätze und Rechenschaftspflicht

Der Verantwortliche ist für die Einhaltung des Art. 5 Abs. 1 EU-DSGVO verantwortlich und muss dessen Einhaltung nachweisen können.

Unser Tipp:

Was sollten Sie bei der Verarbeitung personenbezogener Daten nach Möglichkeit vermeiden?

- Soziale Netzwerke
- Cloud-Dienstleister in Drittstaaten für bspw. Speicherung
- Webseiten-Hosting in Drittstaaten
- Dienste zum Austausch von Nachrichten aus Drittstaaten (z. B. viele beliebte Messenger-Dienste auf dem Mobiltelefon)

Wie gestaltet sich die Kommunikation über Messenger oder digitale Speichermedien?

Der Austausch von Daten über unsichere Dienste, wie WhatsApp, Dropbox oder ähnliches ist nach EU-DSGVO verboten!

Wie Sie Ihre Datenschutzpflichten erfüllen und nachweisen müssen

Das Verarbeitungsverzeichnis

Nach Art. 30 EU-DSGVO sind alle Tätigkeiten zu dokumentieren, bei denen personenbezogene Daten verarbeitet werden. Solche Tätigkeiten können in den unterschiedlichsten betrieblichen Situationen vorkommen (z. B. Erstellung und Veränderung der Kundendatei, Verwaltung der Mitarbeiterakten, etc.). Betriebe, die personenbezogene Daten verarbeiten, sind verpflichtet, sämtliche Verarbeitungsprozesse im sogenannten „Verzeichnis von Verarbeitungstätigkeiten“ zu dokumentieren. Hierdurch soll eine Übersicht über die datenschutzrelevanten Abläufe im Betrieb gegeben werden. Auf Grundlage dieser Übersicht sollen sich Betriebsinhaber über das Ausmaß und die Intensität der betrieblichen Datenverarbeitung bewusst werden. Die Pflicht zur Dokumentation der Datenverarbeitungsprozesse sowie die konkreten Anforderungen an die Dokumentation sind in Art. 30 EU-DSGVO geregelt.

Ein Muster für ein Verarbeitungsverzeichnis entnehmen Sie bitte der Anlage 3. Bei Fragen folgen Sie den Erläuterungen zum Hauptblatt und den Erläuterungen zum Verarbeitungsverzeichnis..

Hinweis:
Sollten Ihre Fragen keine Beantwortung in den Erläuterungen finden, so ist es sinnvoll Ihren Verantwortlichen für IT bzw. den IT-Dienstleister einzubeziehen oder auf die Expertise eines Datenschutzexperten zurückzugreifen.

Datenschutz durch Technik und Organisation bzw. technisch und organisatorischen Maßnahmen (TOM)

Betriebe sind verpflichtet, geeignete technische und organisatorische Maßnahmen (TOM), im angemessenen Rahmen ihrer Möglichkeiten, zur Datensicherheit umzusetzen. Dabei haben sie den Stand der Technik unter Berücksichtigung der Implementierungskosten, der Eintrittswahrscheinlichkeit und dem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen zu beachten. Dabei muss das Sicherheitslevel der Höhe des Risikos entsprechen.

Bei den TOM handelt es sich im Grunde um eine Anlage zum Verarbeitungsverzeichnis, da aus dem Verarbeitungsverzeichnis auf die spezielle Dokumentation der konkreten technischen und organisatorischen Umsetzungsmaßnahmen verwiesen wird.

Eine Checkliste zur Dokumentation der technischen und organisatorischen Maßnahmen (TOM) entnehmen Sie bitte der Anlage 4.

Hinweis:
Die Checkliste dient Ihnen nur als Hilfsmittel zur Beschreibung vorhandener und zum Auffinden der fehlenden Maßnahmen. Sie sollten nur solche Maßnahmen ankreuzen, die Sie auch tatsächlich treffen. Bitte beachten Sie, dass die zu treffenden Maßnahmen für jeden Betrieb individuell zu beurteilen sind. Für TOM gilt ein sogenanntes Verhältnismäßigkeitsprinzip. Demnach müssen personenbezogene Daten nicht unendlich stark geschützt werden, wenn die Maßnahmen dafür wirtschaftlich unangemessen hoch ausfallen würden.

Verantwortlicher & Datenschutzbeauftragter

Der Verantwortliche und der Auftragsverarbeiter setzen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

Haftung & Sanktionen

Nehmen Sie die EU-DSGVO ernst. Sie bildet im Wesentlichen das deutsche Bundesdatenschutzgesetz ab, das ebenfalls zum 28. Mai 2018 auf die EU-DSGVO abgestimmt wurde.

Beachten Sie bitte hier folgende Aspekte:

- Nach der EU-DSGVO drohen bei Verstößen gegen den Datenschutz erhebliche Geldstrafen.
- Jeder an einer Verarbeitung von personenbezogenen Daten beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht-datenschutzkonforme Verarbeitung verursacht wurde. Die Schadenshaftung gilt auch für Ihre Mitarbeiter.
- Die EU-DSGVO führt außerdem für die betroffenen Personen einen Anspruch auf Schadenersatz bei materiellem oder immateriellem Schaden ein.

Eine Verpflichtung auf den Datenschutz für Ihre Beschäftigten entnehmen Sie bitte der Anlage 5.

Hinweis:
Die Verantwortung für die Umsetzung von Datenschutz und Datensicherheit nach den gesetzlichen Vorgaben verbleibt trotz des Einbinden kompetenter Personen weiterhin bei den Unternehmensverantwortlichen.

Muss der Betrieb eine Datenschutzfolgeabschätzung durchführen?

Unter bestimmten Umständen muss die Dokumentation auch eine Datenschutz-Folgenabschätzung enthalten. Maßgebliches Ziel der Datenschutz-Folgenabschätzung ist die systematische Vorabbewertung von Risiken für die Rechte und Freiheiten der Betroffenen, die einzelne Verarbeitungsvorgänge mit sich bringen.

Hinweis:
Eine Datenschutzfolgeabschätzung ist im zahntechnischen Betrieb im Regelfall nicht notwendig.

Gibt es Meldepflichten?

Datenschutzverletzungen, die zu einem Risiko der Rechte und Freiheiten von Betroffenen führen, sind innerhalb von 72 Stunden bei der verantwortlichen Datenschutzbehörde zu melden. In der Regel handelt es sich dabei um die Landesdatenschutzbehörde des Bundeslandes, in dem ein Labor seinen eingetragenen Geschäftssitz hat.

Beispiele:

- Diebstahl von Gesundheitsdaten der Patienten eines zahntechnischen Labors durch einen Hackerangriff
- Diebstahl einer Datensicherungs-Festplatte mit Gesundheitsdaten der Patienten eines zahntechnischen Labors im Rahmen eines Einbruchs
- Verlust eines unverschlüsselten USB-Sticks mit Adress- und Bankdaten von Kunden

Kommt es zu einer Datenschutzverletzung müssen diese und die damit einhergehenden Maßnahmen zur Abhilfe möglichst umfangreich dokumentiert werden.

- Je nach Einzelfall ist zu entscheiden, ob auch die Betroffenen zu informieren sind.
- Ein schriftlich vordefinierter Prozess für die Meldung erleichtert es, bei Bedarf, der Verpflichtung nachzukommen.

Was ist ein Datenschutzbeauftragter?

Unternehmen, die personenbezogene Daten verarbeiten, müssen unter bestimmten Voraussetzungen einen eigenen Datenschutzbeauftragten (DSB) benennen.

Der DSB kann ein Mitarbeiter des Betriebs (intern) oder ein außenstehender Dienstleister (extern) sein.

Unabhängig davon, ob es sich um einen internen oder externen Datenschutzbeauftragten handelt, dürfen nur solche Personen bestellt werden, die

- eine erforderliche Zuverlässigkeit und fachliche Qualifikationen auf den Gebieten Datenschutzrecht und IT-Fachwissen verfügen (diese Begriffe werden im Gesetz nicht näher beschrieben) sowie
- bei der Aufgabenwahrnehmung in keinen Interessenskonflikt geraten können.

Interessenskonflikte bestehen z. B. für Mitglieder der Geschäftsführung, verantwortliche Beschäftigte der EDV oder der Personalabteilung, etc., da diese

Personen für die Datenverarbeitung verantwortlich sind und sich somit als bestellte Datenschutzbeauftragte selbst kontrollieren würden.

Für weitere Informationen über die Aufgaben des Datenschutzbeauftragten folgen Sie dem Link: www.lda.bayern.de/media/info_dsb.pdf

Benötigt der Betrieb einen Datenschutzbeauftragten?

Betriebe haben nur dann einen Datenschutzbeauftragten zu bestellen, wenn sich in der Regel:

- mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

Hinweis:
Es zählen alle Beschäftigten (nicht nur angestellte Mitarbeiter), d. h. auch Mini-Jobber, Praktikanten, Auszubildende, externe Aushilfen usw., die ständig Zugang zur automatisierten Verarbeitung haben.

Was ist die automatisierte Verarbeitung von Daten?

Eine automatisierte Verarbeitung von Daten liegt dann vor, wenn die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen erfolgt. Darunter zählen alle Geräte oder digitale (auch virtuelle) Dienste, die um ein Speichermedium verfügen und im oder für den Betrieb genutzt werden. (Computer, Smartphones, Server aber auch moderne Kopierer, etc.) Auch wenn ein Beschäftigter ständig Zugang zu Mailkonten des Betriebs hat, ist dieser als Person mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt. Das Zugriffsgerät ist dabei unerheblich.

Hinweis:
Derzeit haben mehr als 70 Prozent der Meisterlabore weniger als 9 Beschäftigte. Für diese dürfte gelten, dass sie keinen Datenschutzbeauftragten aus Rechtsgründen benötigen. Bezieht man die vorgenannte Bestimmung nur auf die automatisierte Verarbeitung, dann dürfte sich die Zahl jener Betriebe, die zwingend einen Datenschutzbeauftragten benötigen, sicherlich noch verringern. Das ist allerdings davon abhängig, wie in den nächsten Monaten die verantwortlichen Stellen sich auf eine konkrete Auslegung der Regelung einigen. Teilweise/Vereinzelt wird vertreten, dass zu der Kerntätigkeit der Gesundheits-Handwerke in der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten (Gesundheitsdaten) gehört und deshalb immer ein Datenschutzbeauftragter bestellt werden muss. Dies bedarf jedoch noch der abschließenden Klärung. Die Innungen und der VDZI setzen sich hier für eine Klarstellung ein.

Interner oder externer Datenschutzbeauftragter – Was ist besser?

Die Bestellung des Datenschutzbeauftragten muss in jedem Fall schriftlich erfolgen. Für die Tätigkeit als betrieblicher Datenschutzbeauftragter ist keine bestimmte Ausbildung vorgesehen, jedoch dürfen die Aufgaben eines Datenschutzbeauftragten auch nicht unterschätzt werden.

Ein Musterformular für die Bestellung eines betrieblichen (internen) Datenschutzbeauftragten entnehmen Sie bitte der Anlage 6.

Grundsätzlich ist es gleichgültig, ob ein interner oder externer Datenschutzbeauftragter bestellt wird. Der Vorteil eines internen Datenschutzbeauftragten ist, dass dieser das Unternehmen sowie Geschäftsabläufe und verantwortliche Personen kennt.

Unser Tipp:
Die Wahl des betrieblichen Datenschutzbeauftragten sollte mit Bedacht getroffen werden, da durch den gesetzlichen Sonderkündigungsschutz, ebenso wie durch die Nachwirkung dieses Kündigungsschutzes, die Stellung des betrieblichen Datenschutzbeauftragten insgesamt erheblich gestärkt worden ist und nun mit der Stellung von Betriebsräten vergleichbar ist.

Demgegenüber bietet die Bestellung eines externen Datenschutzbeauftragten den Vorteil, dass dieser von außen objektiv und unbefangen auf das Unternehmen blicken kann. Außerdem genießt der externe Datenschutzbeauftragte, anders als der interne Datenschutzbeauftragte, keinen besonderen Kündigungsschutz.

Auftragsverarbeitung – worauf ist hier zu achten?

Der Dienstleister verarbeitet die Daten für und im Auftrag des Betriebs. Bei der Verarbeitung von personenbezogenen Daten durch Dritte ist der zahntechnische Betrieb für die Einhaltung der Vorschriften im Bereich Datenschutz verantwortlich. Eine Auftragsverarbeitung liegt vor, wenn ein Betrieb zwar personenbezogene Daten für seine Zwecke nutzt, die tatsächliche Verarbeitung dieser Daten aber nicht selbst durchführt, sondern von einem Dienstleister vornehmen lässt.

Beispiele für solche Verarbeitungen:

- ausgelagerter Buchhaltungsservice
- Cloud-Dienste für den Datenaustausch oder zur Speicherung

Wenn Sie eindeutig einen Dritten mit der Verarbeitung personenbezogener Daten beauftragen, etwa bei Personalbuchhaltung durch eine externe Lohnbuchaltung, so ist es sinnvoll und notwendig eine Auftragsverarbeitung schriftlich zu vereinbaren. Hierzu gibt das Muster in der Anlage 7 die notwendigen Hinweise.

Hinweis:
Ob zwischen dem Zahnarzt als Vertragspartner und dem Labor ein Auftragsverhältnis besteht, das die Verarbeitung personenbezogener Daten zum Inhalt hat, hierzu gibt es zum gegenwärtigen Zeitpunkt unterschiedliche Auffassungen und ist mithin noch zu klären.

Auch der Versand einer E-Mail mit personenbezogenen Daten, wie Patientennamen etc., über einen E-Mail-Dienstleister ist eine Verarbeitung durch Dritte.

Muss mit Dienstleistern gesprochen werden?

Es empfiehlt sich das Auftragsverhältnis mit Ihren Dienstleistern zu überprüfen. Am besten sollte eine Vereinbarung zur Auftragsverarbeitung mit jedem Dienstleister getroffen werden. Dafür schreibt die DSGVO keine besondere Form vor, dennoch empfiehlt es sich – allein aus Dokumentations- und Beweisgründen – einen Vertrag in Textform zu schließen. Das Gesetz bezeichnet den Dienstleister als „Auftragsverarbeiter“. Der beauftragende Betrieb wird „Verantwortlicher“ genannt, da er die Daten nutzt und damit trotz Einschaltung eines Dienstleisters auch für die Rechtmäßigkeit der Datenverarbeitung einstehen muss und verantwortlich bleibt. Deshalb haften bei Datenschutzverstößen der auftragsverarbeitende Dienstleister und der Verantwortliche gemeinsam.

Ein Muster für eine Vereinbarung zur Auftragsverarbeitung entnehmen Sie bitte der Anlage 7.

Unser Tipp:
Vermeiden Sie unnötige Probleme und Gefährdungen, indem Sie nach Möglichkeit nur Dienstleister nutzen, die ganz klar dem Datenschutzrecht der EU unterliegen und deren Serverumfeld sich in der EU befindet.

Einfache organisatorische Schritte zu mehr Datensicherheit

Geeignete Sicherheitsmechanismen können verhindern, dass personenbezogene Daten über Kunden, Lieferanten oder Mitarbeiter aus dem EDV-System unkontrolliert entnommen werden.

Datenschutzerklärung von Ihren Mitarbeitern

Lassen Sie eine Datenschutzerklärung von Ihren Mitarbeitern unterschreiben, aus der klar hervorgeht, dass personenbezogene Daten Eigentum des Unternehmens sind und nur in definierten Anwendungsfällen und zu bestimmten Zwecken in einem bestimmten Umfang verwendet werden dürfen. Weisen Sie auf das Datengeheimnis hin und darauf, dass alle Beschäftigten zur Vertraulichkeit und zur Wahrung der Geschäftsgeheimnisse verpflichtet sind.

Informieren Sie auch darüber, dass eine unzulässige Verarbeitung personenbezogener Daten für den Mitarbeiter als Ordnungswidrigkeit oder gar als Straftat verfolgt werden kann.

Definieren Sie klare Anweisungen und Prozesse für Ihre Mitarbeiter und schulen Sie diese darin, wie Datensätze zu erstellen, zu ändern und zu löschen sind. Vermitteln Sie Ihren Mitarbeitern auch die rechtliche Bedeutung eines umfassenden Datenschutzes für sie selbst und für das Unternehmen.

Klare Rechtestrukturen für den Datenzugriff schaffen

Wer darf auf welche Daten zugreifen?
Zur Sicherheit von personenbezogenen Daten sind (programm-)technische Vorkehrungen für

- den Schutz vor Datendiebstahl
- den Schutz vor Missbrauch
- den Schutz vor unberechtigtem Zugriff

sinnvoll und erforderlich. Für alle EDV-Programme in denen personenbezogene Daten verarbeitet werden, sollte es ausreichende programmtechnische Möglichkeiten geben, die Zugriffe zielgerecht einzurichten und die Zugriffe zu protokollieren.

Erst mit einer klaren Regelung über die Einrichtung von Kennwörtern und Richtlinien sorgen Sie für eine effektive Zugriffskontrolle.

Sorgen Sie für klare Rechtestrukturen und sorgen Sie für deren Einhaltung.

Je ausgefeilter und ausgereifter das Rechtesystem Ihrer Programme ist, desto besser und zielgenauer kann der Zugriff auf personenbezogenen Daten für den einzelnen Mitarbeiter gesteuert werden.

Mögliche Rechte-Ebenen sind:

- Rechte für Benutzergruppen,
  (z. B. für unterschiedliche Abteilungen und Hierarchiestufen im Betrieb)
- Rechte auf Program-Module,
  (z. B. nur Auftragsverwaltung, nur Marketing)
- Individuelle Rechte auf die Feldebene,
  (z. B. für Kunden- oder Mitarbeiterdaten)
- Individuelle Rechte auf einzelne Datensätze,
  (z. B. Adressen, Preise, vertrauliche Termine)
- Lese- und Schreibrechte
  (z. B. das Recht zum lesen von Daten oder das Recht diese auch ändern zu dürfen)

Spezielle Rechte sollten explizit für das Löschen von Datensätzen einstellbar ein. Es sollten keine Daten mutwillig oder aus Versehen permanent gelöscht werden können.

Um einem Versehen vorzubeugen, ist beim Löschen von Daten ein 2-stufiger Prozess über den Papierkorb zu empfehlen. Eine ausführliche Dokumentation des betrieblichen Rechtekonzeptes sorgt für mehr Sicherheit und Klarheit.

ANLAGEN

In den Anlagen finden Sie verschiedene Muster zu erforderlichen Erklärungen, Benennungen und Vereinbarungen. Sie sollen beispielhaft, aber realitätsnah, deutlich machen, welche Regelungsinhalte im Rahmen der neuen EU-DSGVO behandelt werden. Wenn Sie Mitglied einer Innung sind, die Mitglied des VDZI ist, dann können Sie sich im Mitgliederbereich auch die Muster als Word-Dokumente zur individuellen Bearbeitung herunterladen.

[Auf Briefbogen des Betriebs]

MUSTER

(ohne Pflicht zur Benennung eines/einer Datenschutzbeauftragten)

Information an den Datengeber

Informationen zur Datenerhebung gemäß Artikel 13 DSGVO

Der/die Musterbetrieb, Musterstraße 1, 12345 Musterstadt, Inhaber Herr Mustermann, erhebt Ihre Daten zum Zweck einer Versorgung mit Zahnersatz, zur Erfüllung seiner/ihrer vertraglichen, vorvertraglichen und gesetzlichen Pflichten.

Die Datenerhebung und Datenverarbeitung ist erforderlich und beruht auf Artikel 6 und 9 DSGVO. Soweit zur Durchführung des Vertrages notwendig oder gesetzlich vorgeschrieben, werden diese Daten an Sozialversicherungsträger, Dienstleistungsträger der gesetzlichen Krankenkassen, Versicherungen, Behörden und die zur Vertragsdurchführung notwendigen Dienstleister oder vergleichbare Dritte weitergegeben. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind. Hierbei sind die steuerrechtlichen (§ 147 AO) sowie handelsrechtlichen (§ 257 HGB) Aufbewahrungsfristen von sechs bzw. zehn Jahren zu beachten.

Sie haben das Recht, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen (Art. 15 DSGVO) sowie bei Unrichtigkeit der Daten die Berichtigung (Art. 16 DS-GVO) oder bei unzulässiger Datenspeicherung die Löschung (Art. 17 DSGVO) der Daten zu fordern. Ebenso steht Ihnen das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) sowie auf Datenübertragbarkeit (Art. 20 DSGVO) zu. Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Sie können unsere/n Datenschutzbeauftragte/n unter datenschutz@musterbetrieb.de oder unter Datenschutzbeauftragte/r c/o Musterbetrieb, Musterstraße 1, 12345 Musterstadt, erreichen.

[Auf Briefbogen des Betriebs]

MUSTER

(ohne Pflicht zur Benennung eines/einer Datenschutzbeauftragten)

Information an den Datengeber

Informationen zur Datenerhebung gemäß Artikel 13 DSGVO

Der/die Musterbetrieb, Musterstraße 1, 12345 Musterstadt, Inhaber Herr Mustermann, erhebt Ihre Daten zum Zweck einer Versorgung mit Zahnersatz, zur Erfüllung seiner/ihrer vertraglichen, vorvertraglichen und gesetzlichen Pflichten.

Die Datenerhebung und Datenverarbeitung ist erforderlich und beruht auf Artikel 6 und 9 DSGVO. Soweit zur Durchführung des Vertrages notwendig oder gesetzlich vorgeschrieben, werden diese Daten an Sozialversicherungsträger, Dienstleistungsträger der gesetzlichen Krankenkassen, Versicherungen, Behörden und die zur Vertragsdurchführung notwendigen Dienstleister oder vergleichbare Dritte weitergegeben. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind. Hierbei sind die steuerrechtlichen (§ 147 AO) sowie handelsrechtlichen (§ 257 HGB) Aufbewahrungsfristen von sechs bzw. zehn Jahren zu beachten.

Sie haben das Recht, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen (Art. 15 DSGVO) sowie bei Unrichtigkeit der Daten die Berichtigung (Art. 16 DS-GVO) oder bei unzulässiger Datenspeicherung die Löschung (Art. 17 DSGVO) der Daten zu fordern. Ebenso steht Ihnen das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) sowie auf Datenübertragbarkeit (Art. 20 DSGVO) zu. Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

[Auf Briefbogen des Betriebs]

MUSTER

Auskunftserteilung des Betriebs an Betroffene

Herrn/Frau
Michael(a) Muster
Mustergasse 1
33333 Musterstadt

Sehr geehrte/r Frau/Herr _____

Sie haben uns um Auskunft darüber gebeten, welche Daten wir zu Ihrer Person gespeichert haben. Sie sind bei uns als _____ (z.B. Kunde/Patient/Interessent) erfasst.

Zur Datenverarbeitung durch unser Unternehmen teilen wir Ihnen mit, dass die Datenerhebung zur Kommunikation mit Ihnen_____ (Weitere Aufzählungen möglich - Bsp: Abgabe von Angeboten, Abrechnung von Leistungen) oder zur Erfüllung von Verträgen erfolgt. Diese Daten haben Sie uns mitgeteilt. Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen erlassen. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung erforderlich sind. Sofern Daten hiervon nicht erfasst sind, werden sie gelöscht, sobald sie für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden. Die Daten werden nicht an Dritte weitergeben. Die über Sie gespeicherten Daten entnehmen Sie bitte der beigefügten Tabelle.

Wir hoffen, dass wir mit den vorstehenden Ausführungen Ihre Fragen hinreichend beantworten konnten. Informieren Sie uns bitte, falls Daten unrichtig sind.

Sie haben das Recht, sich bei der für uns zuständigen Datenschutzaufsichtsbehörde

_____ (zuständiges Landesamt für Datenschutz, Adresse, E-Mail) zu beschweren, falls Sie der Meinung sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt.

Für weitere Auskünfte stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüßen

Firma _____

Anlage

Kunde/Patient/Interessent (bitte wählen)	
Familienname	
Vorname	
Geburtsname	
Geschlecht	
Geburtsdatum	
Staatsangehörigkeit	
Straße	
PLZ	
Wohnort	
UstID	
Kommunikationsdaten	
Telefon	
Handy	
E-Mail	
Bankverbindung	
Bankname	
IBAN-Nummer	
BIC	
Kundenspezifische Auftragsdaten	
z.B. erbrachte Leistung im Zusammenhang mit ZA (XY)	

Muster

Verarbeitungsverzeichnis

Hauptblatt

Angaben zum Verantwortlichen, Art. 30 Abs. 1 a) DSGVO

1. Verantwortlicher (=Firma/Legaleinheit)
Zahntechnik Mustermann, Musterstraße 17-21, 12345 Musterstadt

2. Gesetzlicher Vertreter (= Geschäftsführung/ Betriebsinhaber)
Herr Otto Mustermann, Musterstraße 17-21, 12345 Musterstadt

3. Datenschutzbeauftragter (soweit erforderlich; vgl. Information bei Erhebung Daten)

Name: Frau Anja Mustermann

Anschrift: Musterstraße 17-21, 12345 Musterstadt

E-Mail: datenschutzbeauftragter@zahntechnik-mustermann.de

Tel.: 01234/ 123456-34

4. Zuständige Aufsichtsbehörde
Landesbeauftragter für Datenschutz und Informationsfreiheit

Verpflichtende Meldung des Datenschutzbeauftragten bereits erfolgt
(soweit Datenschutzbeauftragter erforderlich)

☒ Ja

☐ Nein

5. Regelungen zur Datensicherheit
technische/organisatorische Maßnahmen (siehe Anlage)

6. Sachverhalte zu Drittstaatenübermittlung
Findet nicht statt.

Erläuterungen zum Hauptblatt

Nr. 1	Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO) Angaben: Name/Firma, ladungsfähige Anschrift
Nr. 2	Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter Angaben: Namen der geschäftsführenden Personen *Gegebenenfalls kann hier einfach ein Link auf das Impressum der Webseite des Betriebs eingetragen werden.*
Nr. 3	Vom Verantwortlichen bestellter Datenschutzbeauftragter (sofern ein Datenschutzbeauftragter bestellt wurde) Angaben: Name, Kontaktdaten
Nr. 4	Die Meldung der Kontakt-Informationen des Datenschutzbeauftragten (Funktions-)E-Mail-Adresse und Telefonnummer sind Pflichtangaben.
Nr. 5	Gegebenenfalls Verweise auf übergreifende Regelungen (*falls solche existieren, die grundsätzlich alle Verarbeitungen* betreffen) Der Verweis auf übergreifende Regelungen an dieser Stelle entbindet nicht von der Dokumentation von ggf. erforderlichen Abweichungen zu den einzelnen Verarbeitungstätigkeiten. Verweis z.B. auf ein IT-Sicherheitskonzept, das alle Verarbeitungstätigkeiten einschließt. Eventuell auch Verweise auf relevante Dokumente eines ISMS nach ISO27001.
Nr. 6	Ein Verweis zur Regelungen zur Drittstaatenübermittlung ist hier sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen hierdurch geregelt werden, z.B. durch BCR.

Verzeichnis von Verarbeitungstätigkeiten

☒ Ersterstellung

☐ Änderung eines bestehenden Verzeichnisses

Erstellungsdatum: xx.xx.2018
Bezeichnung der Verarbeitungstätigkeit: Führen eines zahntechnischen Labors

I. Angaben zur Verantwortlichkeit, Art. 30 Abs. 1 b) DSGVO

1. Verantwortlicher Fachbereich/verantwortliche Führungskraft
Herr Mustermann

2. Bei gemeinsamer Verantwortlichkeit:
Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen

II. Angaben zur Verarbeitungstätigkeit

3. Risikobewertung
Besteht bei der Verarbeitung ein hohes Risiko für die betroffenen Personen?

☒ Nein

☐ Ja

Wenn ja, dann Durchführung einer Datenschutz-Folgenabschätzung erforderlich (Art. 35 DSGVO). Datenschutz-Folgenabschätzung als separate Anlage beifügen.

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

Organisation von Geschäftskontakten und Bestandskunden
Versorgung mit Zahnersatz
Durchführung von Verträgen

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit

Art. 6 sowie Art. 9 DSGVO

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO

6.1. Betroffene Personengruppen	6.2. Kategorien personenbezogener Daten
Kunden, Geschäftspartner Arbeitnehmer	Gesundheitsdaten Name, Vorname, Adressdaten, (elektronische) Kontaktdaten, Gegenstand des Auftrags

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, Art. 30 Abs. 1 d) DSGVO

7.1. Interne Empfänger	Mitarbeiter (Meister, Gesellen, Auszubildende, sonstige Mitarbeiter)
7.2. Externe Empfänger	Auftraggeber, Sozialversicherungsträger; Dienstleistungsträger der gesetzlichen Krankenkassen; Finanzbehörden
7.3. Vertragliche Dienstleister (Vertrag der Auftragsdatenverarbeitung als Anlage beifügen)	Ggf. beauftragte Abrechnungsdienstleister; Rechenzentren; zahntechnische Labore; Fräszentren; Hersteller, etc.

8. Datenübermittlungen in Drittländer oder an internationale Organisationen, Art. 30 Abs. 1 e) DSGVO

☒ Nein

☐ Ja

Wenn ja, dann: Name des Drittlandes / der internationalen Organisation (DSGVO):

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien, Art. 30 Abs. 1 f) DSGVO

Die Daten werden gelöscht, wenn sie für die Erfüllung des Versorgungszwecks (siehe Nr. 4) nicht mehr erforderlich und die gesetzlichen Aufbewahrungsfristen erloschen sind.

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO

Siehe Anlage „technische und organisatorische Maßnahmen“ (betriebsinternes IT-Sicherheitskonzept XY)

10.1 Art der eingesetzten DV-Anlagen und Software

_____

(Siehe betriebsinternes IT-Sicherheitskonzept XY)

10.2 Konkrete Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO

_____

(Siehe betriebsinternes IT-Sicherheitskonzept XY)

----- optionale Angaben ----

Weitere Dokumentationen zur Verarbeitungstätigkeit

----- Ende optionale Angaben----

Erläuterungen zum Verarbeitungsverzeichnis

Nr. 1	Eindeutige Bezeichnung der dokumentierten Verarbeitung/ Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen geläufige Bezeichnung des Fachprozesses gewählt werden. Beispiele: - Allgemeine Kundenverwaltung - Customer-Relationship-Management (CRM)
	Nach der Unternehmensorganisation für die konkrete Verarbeitungstätigkeit verantwortlicher Fachbereich/verantwortliche Führungskraft (*sofern möglich und sinnvoll, zumindest als Funktionsbezeichnung*)
Nr. 2	Falls mehrere Verantwortliche gemeinsam für die Verarbeitungstätigkeiten verantwortlich sind, bspw. innerhalb einer Unternehmensgruppe, sind hier Name und Kontaktdaten des/der weiteren Verantwortlichen anzugeben (Firma/ladungsfähige Anschrift; Art. 30 Abs. 1 a) DSGVO, Art. 26 Abs. 1 DSGVO).
Nr. 3	Es ist zu bewerten, ob die Datenverarbeitung ein hohes Risiko für die Personen birgt, deren Daten verarbeitet werden. Ein hohes Risiko liegt u.a. dann vor, wenn sehr viele Personen von der Datenverarbeitung betroffen sind. Das gleiche gilt, wenn besonders schutzwürdige Daten (z.B. Gesundheitsdaten) umfangreich verarbeitet werden. Die Erwägungsgründe der DSGVO bewerten die Verarbeitung von Patientendaten durch einen einzelnen Betrieb des Gesundheitswesens dabei nicht als „umfangreich“.
Nr. 4	Eine Verarbeitungstätigkeit kann mehrere Teil-Geschäftsprozesse zusammenfassen. Dementsprechend kann eine Verarbeitung auch mehrere Zwecke umfassen, so dass auch mehrere Zweckbestimmungen angegeben werden können.
Nr. 5	Die Nennung der einschlägigen Rechtsgrundlage ist für Rechenschaftspflichten und die Gewährleistung von Transparenzpflichten ggü. den betroffenen Personen notwendig. Die Rechtsgrundlage können z.B. eine gesetzliche Vorschrift oder eine Einwilligung durch den Betroffenen sein.
Nr. 6	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO
Nr. 6.1	Als betroffene Personengruppen kommen beispielsweise Kunden, Interessenten, Arbeitnehmer, Schuldner, Versicherungsnehmer usw. in Betracht.
Nr. 6.2	Den einzelnen Personengruppen sind die jeweils auf sie bezogenen verwendeten Daten oder Datenkategorien zuzuordnen. Damit sind keine personenbezogenen Daten, sondern "Datenbezeichnungen"/Datenkategorien gemeint (z.B. „Adresse“, „Geburtsdatum“, „Bankverbindung“). Werden solche Datenkategorien angegeben, so müssen diese so konkret wie möglich sein. Nicht ausreichend sind etwa Angaben wie „Kundendaten“ oder Ähnliches. Beispiele: - Kunden: Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax-und E-Mail-Daten), Geburtsdatum, Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließlich Kundenentwicklung, Produkt- bzw. Vertragsinteresse, Statistikdaten, Abrechnungs- und Leistungsdaten, Bankverbindung - Beschäftigtendaten (Lohn und Gehalt): Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, etc.

Nr. 7	Empfängerkategorien sind insbesondere Sozialversicherungsträger und beauftragte Abrechnungsdienstleister sowie andere am Prozess beteiligte weitere Stellen des Unternehmens oder andere Gruppen von Personen oder Stellen, die Daten – ggf. über Schnittstellen – erhalten z.B. in den Prozess eingebundene Angehörige von Gesundheitsberufen, Vertragspartner, Kunden, Behörden, Versicherungen, sowie sonstige Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Hersteller, Reparaturfirmen, Otoplastiklabore, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.
Nr. 8	Drittländer sind solche außerhalb der EU/des EWR Beispiele für internationale Organisationen: Institutionen der UNO, der EU. Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren, Art. 49 Abs. 1. UAbs. 2 DSGVO.
Nr. 9	Anzugeben sind hier die konkreten Aufbewahrungs-/Löschfristen, die in Verarbeitungstätigkeiten implementiert sind, bezogen auf einzelne Verarbeitungsschritte, falls unterschiedlich. Es reicht in der Regel aus, darauf zu verweisen, dass die Daten gelöscht werden, wenn der Versorgungszweck erfüllt ist.
Nr. 10	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO.
Nr. 10.1	Optional kann an dieser Stelle eine knappe Beschreibung der technischen Infrastruktur wie der technischen und organisatorischen Sicherheitsmaßnahmen angegeben werden, um ein besseres Verständnis der allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen (siehe 10.2.) zu ermöglichen.
Nr. 10.2	Soweit sich die technischen und organisatorischen Maßnahmen schon aus vorhandenen Sicherheitsrichtlinien/Konzepten/Zertifizierungen ergeben, ist ein konkreter Verweis hierauf ausreichend.
Optional	Im Hinblick auf die vielfältigen Nachweispflichten, denen das Unternehmen im Datenschutz unterliegt, kann es sinnvoll sein, weitere Aspekte zur Verarbeitungstätigkeit zu dokumentieren. Diese sind nur intern zu verwenden. Zu diesen zusätzlichen Dokumentationen, die sinnvollerweise hier erfolgen, gehören z. B. • *Angaben zur Zusammenstellung der Informationspflichten (insb. Art. 13, 14 DSGVO) (Muster: Information bei Erhebung von Daten beim Betroffenen)* • *Verträge mit Dienstleistern (Art. 28 DSGVO)* • *Vereinbarungen zur gemeinsamen Verantwortung (Art. 26 DSGVO)* • *Eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen* • *durchgeführte Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten (Art. 35 DSGVO)*

[Auf Briefbogen des Betriebs]

MUSTER

Technische und organisatorische Maßnahmen

1. Organisatorische Maßnahmen

- ☐ Ist ein betrieblicher Datenschutzbeauftragter bestellt?
- ☐ Nein
- ☐ Ja
  Name: .....
  Funktion: .....
  E-Mail: .....
  Telefon: .....
- ☐ Mitarbeiter wurden nachweislich über Datenschutzrecht und Datensicherheit geschult.
- ☐ Alle Mitarbeiter sind nachweislich auf das Datengeheimnis, ggf. auf das Fernmeldegeheimnis, verpflichtet.
- ☐ Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen (z.B. technisch unterstützt oder durch Externe).
- ☐ Ein Datensicherheitskonzept/ Informationssicherheitsmanagement ist vorhanden.
- ☐ Ein Datenschutzkonzept ist vorhanden.
- ☐ Eine Auditierung/Zertifizierung ist vorhanden (Prüfung der Einhaltung am _____und Bestätigung s. Anlage ____).
- ☐ Verhaltensregeln nach Art. 40 DSGVO sind vorhanden (Unterwerfung am _____und Bestätigung s. Anlage ____).

2. Vertraulichkeit

a) Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden.

- ☐ Schriftliche Zutrittsregelungen zum Betreten des Rechenzentrums/der Räume mit DV-Anlagen sind vorhanden
- ☐ Alarmanlage
- ☐ Automatisches Zutrittskontrollsystem, Ausweisleser
- ☐ Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)
- ☐ Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)
- ☐ Sicherheitsschlösser
- ☐ Chipkarten-/Transponder-Schließsystem
- ☐ Biometrie (Fingerabdrücke o. ä.)
- ☐ Manuelles Schließsystem
- ☐ Schranken/Vereinzelungsanlagen (Drehkreuze o. ä.)
- ☐ Magnetschleusen

- ☐ Werkschutz/Pförtner
- ☐ Empfang mit Anmeldung
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Lichtschranke/Bewegungsmelder
- ☐ Feuerfeste Türen
- ☐ Absicherung von Gebäudeschächten
- ☐ Fenstervergitterung
- ☐ Panzerglas
- ☐ Videoüberwachung der Zugänge

b) *Zugangs- und Benutzerkontrolle*

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☐ Passwortvergabe
  Länge des Passworts: ... Zeichen
  Wechselfristen: ... Wochen/Monate
  Anzahl der Fehleingaben: ...
- ☐ Chipkarte mit PIN/Passwort
- ☐ Authentifikation mit Benutzername/Passwort
- ☐ Biometrisches Merkmal mit PIN/Passwort
- ☐ Einsatz von VPN-Technologie
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☐ Verschlüsselung von mobilen Datenträgern

c) *Zugriffskontrolle*

Maßnahmen, die gewährleisten, dass Personen nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- ☐ Schriftliches Berechtigungskonzept vorhanden
- ☐ Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen
- ☐ Verwaltung der Rechte durch System-Administrator
- ☐ Anzahl der Administratoren auf das "Notwendigste" reduziert
- ☐ Gesicherte Nutzung von USB-Schnittstellen
- ☐ Automatische Sperrung des Arbeitsplatzes
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ Die Protokolle werden ausgewertet, zeitlicher Abstand: ....
- ☐ Einsatz von Akten-/Datenträgervernichtern bzw. Dienstleistern unter Beachtung von DIN 66399
- ☐ Verschlüsselung von Datenträgern
- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ Ordnungsgemäße Vernichtung von Datenträgern
- ☐ Löschungskonzept für Daten
- ☐ Protokollierung der Vernichtung

d) *Transport- und Übertragungskontrolle*

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen *Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft werden*

kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ Firewall: Die nach dem Stand der Technik erforderlichen Firewall-Technologien sind implementiert und werden auf dem aktuellen Stand gehalten
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung
- ☐ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☐ Protokollierung von Übermittlungen
- ☐ Erstellen einer Übersicht von Datenträgern, Aus- und Eingang
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- ☐ Sicherung von Datenträgertransporten (verschließbarer Transportbehälter), auch für Papier

e) *Auftragskontrolle*

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- ☐ Vorhandene Vereinbarungen zur Auftragsverarbeitung
- ☐ Kontrolle der Vertragsausführung
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Regelung zu Wartungen (speziell Fernwartung)

3. Integrität

a) *Eingabekontrolle/Verarbeitungskontrolle*

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☐ Protokollauswertungsroutinen/-systeme vorhanden
- ☐ Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden

b) *Dokumentationskontrolle*

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

- ☐ Führung eines Verarbeitungsverzeichnisses
- ☐ Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration
- ☐ Zulässigkeit eines Datentransfers in Drittländer ist gegeben

4. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und im Störfall wieder hergestellt werden können.

- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Überspannungsschutz
- ☐ Schutz gegen Umwelteinflüsse (Sturm, Wasser)
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☐ Testen von Datenwiederherstellung
- ☐ Klimaanlage in Serverräumen
- ☐ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuerlöschgeräte in Serverräumen
- ☐ Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort)
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ Virenschutzsystem
- ☐ Spiegelung von Festplatten (z. B. RAID-Verfahren)
- ☐ Konzept für Katastrophenfall vorhanden

5. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- ☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Trennung von Produktiv- und Testsystem
- ☐ Festlegung Technologie von Datenbankrechten
- ☐ Trennung von Daten verschiedener Auftraggeber

[Auf Briefbogen des Betriebs]

MUSTER

Verpflichtung auf den Datenschutz

Ich, Frau/Herr _____ wurde heute von meinem Arbeitgeber über die datenschutzrechtlichen Bestimmungen informiert.

Es wurde mir insbesondere erläutert, dass es untersagt ist Patienten- bzw. Kundendaten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Sie dürfen ausschließlich insoweit erhoben, verarbeitet oder genutzt werden, als sie für die Durchführung des Kundenauftrages notwendig sind.

Mir wurde ferner erläutert, dass ich über sämtliche mir im Zusammenhang mit meiner Tätigkeit bekannt gewordenen Daten strengstes Stillschweigen zu bewahren habe. Diese Verschwiegenheitspflicht besteht gegenüber jedermann, auch gegenüber Familienangehörigen, Arbeitskollegen, soweit eine Mitteilung nicht aus dienstlichen Gründen zu erfolgen hat.

Meine Verschwiegenheitspflicht besteht auch nach der Beendigung des Beschäftigungsverhältnisses fort.

Auch sämtliche betriebsinterne Vorgänge unterliegen meiner Verschwiegenheitspflicht.

Verstöße gegen das Datengeheimnis können nach §§ 41 ff. BDSG 2018 sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe bzw. Geldbußen geahndet werden.

In der Verletzung des Datengeheimnisses kann zugleich eine Verletzung arbeitsrechtlicher Schweigepflichten mit entsprechenden arbeitsrechtlichen Konsequenzen liegen.

_____, _____
(Ort) (Datum)

_____, _____
(Betriebsleiter/in) (Arbeitnehmer/in)

[Auf Briefbogen des Betriebs]

MUSTER

Bestellung eines/r betrieblichen Datenschutzbeauftragten

Herrn/Frau
Michael(a) Muster
Mustergasse 1
33333 Musterstadt

Sehr geehrte/r Frau/Herr _____,

ich/wir benennen Sie mit sofortiger Wirkung zur/m Datenschutzbeauftragten gemäß Artikel 37 Abs. 1 b) und c) EU-Datenschutzgrundverordnung (DSGVO) in Verbindung mit
§ 38 Bundesdatenschutzgesetz (BDSG). In Ihrer Funktion als Datenschutzbeauftragte/r sind Sie der Geschäftsleitung unmittelbar unterstellt.

Zuständiges Mitglied der Geschäftsleitung ist

_____

Ihre Aufgaben als Datenschutzbeauftragte/r ergeben sich aus den Artikeln 37 bis 39 DSGVO sowie § 38 BDSG. In Anwendung Ihrer Fachkunde auf dem Gebiet des Datenschutzes sind Sie weisungsfrei. Bei der Erfüllung Ihrer Aufgaben sind Sie an die Wahrung der Geheimhaltung und der Vertraulichkeit gebunden. Über Ihre Tätigkeit werden Sie der Geschäftsleitung laufend Bericht erstatten.

Erforderliche Organisationsanweisungen schlagen Sie der Geschäftsleitung vor.

_____

Ort, Datum *Unterschrift Geschäftsleitung*

Mit der Benennung bin ich einverstanden

_____

Unterschrift Datenschutzbeauftragte/r

[Auf Briefbogen des Betriebs]

MUSTER

Auftragsverarbeitung – Hinweise und Formulierungshilfen

Vereinbarung

zwischen dem/der

_____

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

_____

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

Hinweis:

Der Gegenstand und die Dauer des Auftrags müssen individuell mit dem Auftragsdatenverarbeiter verhandelt und festgelegt werden.

Formulierungsvorschlag:

Gegenstand:

„Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung _____ vom _____ auf die hier verwiesen wird."

oder

„Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer_____."
(mit Definition der Aufgaben)

Dauer:

„Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung."

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

„Der Auftrag wird zur einmaligen Ausführung erteilt."

oder

„Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum _____."

oder

„Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von _____ zum _____ gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt."

Ein vollständig ausformuliertes Muster ist wegen der Individualität der Vereinbarungen an dieser Stelle nicht möglich.

2. Umfang, Art und Zweck der Datenverarbeitung

Formulierungsvorschlag:

„Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im sachlichen und zeitlichen Rahmen dieses Auftrages sowie nach Weisung des Auftraggebers. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

Die Verarbeitung der Daten auch durch Unterauftragnehmer findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt.

Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

3. Technische und organisatorische Maßnahmen

Formulierungsvorschlag:

„Der Auftragnehmer wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den gesetzlichen Anforderungen genügen. Hierbei sind die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Die technisch-organisatorischen Maßnahmen des Auftragnehmers sind gesondert zu diesem Vertrag festzulegen und sind Bestandteil des Vertrags.

Der Auftragnehmer gewährleistet ein Verfahren zur Überprüfung der technischen und organisatorischen Maßnahmen. Er ist verpflichtet, die technischen und organisatorischen Maßnahmen an den Stand der Technik anzupassen, soweit dies erforderlich und wirtschaftlich zumutbar ist. Der Auftraggeber ist über wesentliche Änderungen vorab zu informieren. Die Änderungen sind schriftlich niederzulegen und werden Vertragsbestandteil. Vorschläge des Auftraggebers für Änderungen hat der Auftragnehmer zu prüfen. Der Auftraggeber ist über das Ergebnis zu informieren.

Beauftragt der Auftragnehmer zur Erfüllung seiner vertraglichen Pflichten einen Unterauftragnehmer, stellt er sicher, dass die erforderlichen technischen und organisatorischen Maßnahmen vom Unterauftragnehmer getroffen werden und dem Stand der Technik entsprechen.“

4. Berichtigung, Sperrung und Löschung von Daten, Auskunft über Daten

Formulierungsvorschlag:

„Der Auftragnehmer hat die Daten nach Weisung des Auftraggebers zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Sperrung oder Löschung seiner Daten wendet, leitet der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiter. Das gleiche gilt für Auskunftsersuche."

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Formulierungsvorschlag:

„Der Auftragnehmer ist verpflichtet, das Datengeheimnis sowie etwaige berufliche Verschwiegenheitsverpflichtungen zu wahren. Er hat bei der Verarbeitung ausschließlich Beschäftigte einzusetzen, die entsprechend verpflichtet und geschult sind. Er hat insbesondere sicherzustellen, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung dieses Vertrages betraut sind, sorgfältig ausgewählt werden, die gesetzlichen Datenschutzbestimmungen beachten und die vom Auftraggeber erlangten Informationen nicht unbefugt an Dritte weitergeben oder anderweitig verwerten.

Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für sämtliche vertragsrelevanten Angelegenheiten des Datenschutzes.

Der Auftragnehmer hat Frau/Herrn _____
als betrieblichen Datenschutzbeauftragten bestellt.
(nur wenn ein Datenschutzbeauftragter bestellt wurde)

Der Auftragnehmer ist verpflichtet, ein Verarbeitungsverzeichnis gemäß Art. 30 Abs. 2 DSGVO zu führen. Der Auftragnehmer gewährt dem Landesdatenschutzbeauftragten Zugang zu den Arbeitsräumen und unterwirft sich der Kontrolle nach Maßgabe des Landesdatenschutzgesetzes in seiner jeweiligen Fassung. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontroll- und Ermittlungshandlungen der Aufsichtsbehörde."

6. Unterauftragsverhältnisse

Formulierungsvorschlag:

„Der Auftraggeber genehmigt die gesondert aufgelisteten Unterauftragsverhältnisse, die der Auftragnehmer vor Abschluss dieser Vereinbarung begründet hat. Über Änderungen hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Abschluss neuer Unterauftragsverhältnisse bedarf der vorherigen Zustimmung des Auftraggebers.

Der Auftragnehmer hat dem Unterauftragnehmer dieselben Pflichten aufzuerlegen, die er selbst gegenüber dem Auftraggeber zu erfüllen hat. Der Unterauftragnehmer ist sorgfältig auszuwählen. Der Auftragnehmer haftet gegenüber dem Auftraggeber vollumfänglich für Datenverstöße seiner Unterauftragnehmer."

7. Kontrollrechte des Auftraggebers

Formulierungsvorschlag:

„Der Auftraggeber hat das Recht, vor Beginn und während der Datenverarbeitung die Einhaltung der vom Auftragnehmer sowie von den Unterauftragnehmern getroffenen technischen und organisatorischen Maßnahmen zu kontrollieren oder von zu benennenden Prüfern kontrollieren zu lassen. Das Ergebnis ist zu dokumentieren.

Der Auftragnehmer gewährleistet die Möglichkeit zur Kontrolle. Hierzu weist er dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO nach. Der Nachweis kann durch Vorlage aktueller Testats oder durch Berichte unabhängiger Prüfer (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Datenschutzauditoren, Qualitätsauditoren) erbracht werden.

Haben sich der Auftragnehmer und die von ihm beauftragten Unterauftragnehmer Verhaltensregeln unterworfen oder ein Zertifizierungsverfahren erfolgreich durchlaufen, sind sie verpflichtet, dem Auftraggeber dies nachzuweisen. Zertifikate sind zu aktualisieren.

Der Auftraggeber ist berechtigt, Stichprobenkontrollen durchzuführen. Diese sind anzukündigen. Würde die Ankündigung den Zweck der Prüfung gefährden oder besteht ein dringender Anlass zur Kontrolle, ist eine Ankündigung entbehrlich."

8. Mitteilung bei Verstößen

Formulierungsvorschlag:

„Der Auftragnehmer meldet dem Auftraggeber unverzüglich sämtliche Verstöße gegen Pflichten aus diesem Vertrag. Dies gilt insbesondere bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung bzw. zum Ausschluss möglicher nachteiliger Folgen für die Betroffenen zu ergreifen."

9. Weisungsbefugnis des Auftraggebers

Formulierungsvorschlag:

„Der Auftraggeber ist berechtigt, dem Auftragnehmer jederzeit Weisungen zu erteilen, insbesondere hinsichtlich der Art, des Umfangs und des Zeitpunkts der Verarbeitung von Daten. Die Weisungen des Auftraggebers erfolgen in Textform.

Erachtet der Auftragnehmer eine Weisung des Auftraggebers als rechtswidrig, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Er ist berechtigt, die Durchführung der Weisung auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Erteilt der Auftraggeber Einzelweisungen bzgl. des Umgangs mit personenbezogenen Daten, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, z.B. Änderungen der technischen und organisatorischen Maßnahmen, werden sie als Antrag auf Leistungsänderung behandelt."

10. Löschung von Daten und Rückgabe von Datenträgern

Formulierungsvorschlag:

„Der Auftragnehmer hat dem Auftraggeber sämtliche in seinen Besitz befindlichen personenbezogenen Daten, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, unverzüglich nach Erfüllung des Vertrags oder nach Aufforderung durch den Auftraggeber, spätestens mit Beendigung der Zusammenarbeit auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Ein Zurückbehaltungsrecht ist ausgeschlossen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind vom Auftragnehmer entsprechend der geltenden Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren."

VERBAND DEUTSCHER ZAHNTECHNIKER INNUNGEN

VDZI

QUICK-CHECK ZUR EU-DSGVO

- ☑ *Bewusstsein schaffen für das Thema Datenschutz*
- ☑ *Schulen Sie Ihre Mitarbeiter*
- ☑ *Informationspflichten und Betroffenenrechte berücksichtigen*
- ☑ *Verzeichnis über die Verarbeitungstätigkeiten anlegen*
- ☑ *Technische und organisatorische Maßnahmen (TOM) planen, prüfen und dokumentieren*
- ☑ *Notwendige Prozesse festlegen und dokumentieren*
- ☑ *Datenschutzbeauftragten falls nötig benennen und einbinden*