Vertrag zur Auftragsverarbeitung

zwischen der
……..
……..
……..

- nachstehend Auftraggeber genannt –
und

UROWL Dienstleistungsgesellschaft für ambulante Urologie mbH
Stockweg 9
45481 Mülheim

- nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem Dienstleistungsvertrag über die Erbringung von Leistungen zur Tumordokumentation und Krebsregistermeldung, auf die hier verwiesen wird (im Folgenden Dienstleistungsvertrag).

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Dienstleistungsvertrags.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben im Dienstleistungsvertrag. Die Auftragserbringung und Verarbeitung erfolgt mit den vom Auftraggeber bereitgestellten Hard-/Software. Hierfür erhält der Auftragnehmer entsprechende und für den Auftrag erforderliche Zugriffsberechtigungen. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in Räumlichkeiten der Klinik und/oder über einen von der IT Abteilung bereitgestellten VPN Zugang /Citrix oder Fernzugang (z.B. TemViewer) mit einem zugelassenen Endgerät gemäß Anhang 1 dieser Vereinbarung vom Arbeitsplatz des Auftragnehmers statt.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

○Patientendaten

- Stammdaten
- Name/Vorname
- Geburtsdatum
- Geschlecht
- Alter
- Anschrift
- Kontaktdaten (Telefon)
- Ethnische Zugehörigkeit
- Titel

Identifizierende Daten

- Patient-ID aus Informationssystem

Administrative Daten

- Versichertenart (privat oder gesetzlich versichert
- Krankenversicherung/Krankenkasse sowie Versichertenart
- Ggf. Krankenversicherten-Nr. sowie Gültigkeit

Medizinische Daten

- Physiologische Auffälligkeiten

Klinische Daten aus Anamnese, Diagnose, Therapie

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

○ Patienten

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer erkennt die Umsetzung und Einhaltung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung an.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet sie insbesondere die Einhaltung folgender Vorgaben:
a) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO.
b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei dem Auftragnehmer ermittelt. Nach Art. 28 Abs. 3 der Datenschutz-Grundverordnung (DS-GVO) verpflichtet sich der Auftragnehmer, den Auftraggeber unverzüglich zu informieren, falls eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt. Der Auftragnehmer wird den Auftraggeber dabei unterstützen, angemessene Maßnahmen zur Sicherung der Rechte der betroffenen Personen zu ergreifen.
d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung bei dem Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in ihrem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

6. Unterauftragsverhältnisse

Der Auftragnehmer ist befugt, die in Anlage 2 dieses Vertrags aufgeführten Unterauftragnehmer zur Datenverarbeitung im Auftrag einzusetzen. Unter bestimmten Bedingungen ist ein Wechsel von Unterauftragnehmern oder die Beauftragung zusätzlicher Unterauftragnehmer zulässig.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer jederzeit Überprüfungen zu diesen Vertragsinhalten durchzuführen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigten der Auftraggeber unverzüglich (mind. Textform).

10. Haftung

Es gelten die Regelungen des Dienstleistungsvertrags.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt.
(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Dienstleistungsvertrags – hat der Auftragnehmer sämtliche in ihrem Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten.

Ort, den
UROWL GmbH , Auftragnehmer
Vertreten durch den GF
Holger Warnat

Auftraggeber, Vertreter
Praxisstempel

Anlagen

Auftraggeber, Vertreter
Anlage 1 TOM's (technische und organisatorische Maßnahmen)
Anlage 2 Unterauftragsnehmerverhältnisse
Anlage 3 Verpflichtung zur Wahrung der Vertraulichkeit

Anlage 1

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

Der Auftragnehmer (UROWL) sichert zu, folgende technische und organisatorische Maßnahmen getroffen zu haben:

A. Maßnahmen zur Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.
Beschreibung der Pseudonymisierung: die Patientenidentifikationsnummer, gekoppelt mit der Melder-Identifikationsnummer lässt über das Meldeportal einen Rückschluss auf den Patienten zu in der jeweiligen Praxis/Klinik. Die Kommunikation über Patienten erfolgt mit den Landeskrebsregistern ausschließlich über die Nachrichtenfunktion im Meldeportal und dem jeweiligen Zugang für den Melder, auch telefonisch oder postalisch zum Melder

B. Maßnahmen zur Verschlüsselung

Maßnahmen oder Vorgänge, bei denen ein klar lesbarer Text / Information mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird:
Eine Verschlüsselung der Daten wird im Meldeprozess an die Landeskrebsregister von diesen vorgenommen.

C. Maßnahmen zur Sicherung der Vertraulichkeit

1. Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren:
Beschreibung des Zutrittskontrollsystems:
Die Dokumentation findet beim Kunden vor Ort oder „remote“ statt. Ein Zutrittskontrollsystem wird in der jeweiligen Praxis/Klinik koordiniert. Am „remote“-Arbeitsplatz ist der Arbeitsplatz/-raum geschlossen und kann unabhängig vom Rest des Hauses genutzt werden. Es wird sichergestellt, dass Unbefugte keinen Zugang zu personenbezogenen Daten erhalten.

2. Zugangskontrolle

Um Zugriff auf das System zu erhalten, müssen der Auftragnehmer und seine Partner über eine entsprechende Zugangsberechtigung verfügen. Die Benutzerberechtigungen werden von einem oder mehreren Administratoren des Auftraggebers vergeben. Die Zugänge werden zentral vom Systemadministrator des Auftraggebers verwaltet und regelmäßig überprüft.
Der Auftraggeber steuert alle Nutzerzugänge zu den Services des Auftragnehmers über die Software selbst. Die Einrichtung der Zugänge und alle Änderungen werden protokolliert. Der Login erfolgt mit einem Benutzernamen und Passwort. Es ist nicht zwingend erforderlich, das Passwort regelmäßig zu ändern. Die Software sieht standardmäßig eine Zweifaktorauthentifizierung vor, die vom Auftraggeber nur auf ausdrücklichen Wunsch deaktiviert werden kann. Alle Analyse- und Entwicklungsaktivitäten finden ausschließlich auf den Servern des Unterauftragnehmers statt. Die technische Möglichkeit, einzelne oder mehrere Datensätze (Rohdaten) auf lokale Computer zu kopieren, ist unterbunden.
Alle Server und Client-Systeme, die bei der Erbringung von Leistungen für den Auftraggeber verwendet werden, sind durch Firewalls geschützt. Diese werden regelmäßig gewartet und mit aktuellen Updates und Patches versorgt.

3. Zugriffskontrolle

Um sicherzustellen, dass nur berechtigte Personen auf die personenbezogenen Daten zugreifen können und die Daten während der Verarbeitung, Nutzung und Speicherung vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen geschützt sind, werden folgende Maßnahmen ergriffen:
Der Zugriff auf die Arbeits-Hardware erfolgt nur durch Eingabe eines Passworts. Datensicherungen werden regelmäßig auf einer externen Festplatte erstellt und in einem feuer- und zugriffssicheren Safe aufbewahrt. Auch alle vertraglichen Unterlagen in Papierform werden sicher verwahrt.
Die Vergabe von Berechtigungen für IT-Systeme und Applikationen des Auftragnehmers erfolgt nach dem Need-to-know-Prinzip. Nur Personen, die für die Wartung, Pflege oder Entwicklung der Daten, Anwendungen oder Datenbanken zuständig sind, erhalten Zugriffsrechte. Der Zugriff dieser Mitarbeiter ist auf die für ihre Aufgaben erforderlichen Daten und Tätigkeiten beschränkt.
In Ausnahmefällen ermöglicht der Unterauftragnehmer autorisierten Personen den Zugriff auf aggregierte Ergebnisse durch einen speziell regulierten Zugriffsmechanismus. Diese Regelung gilt für alle Ebenen der Software. Zugriffe auf Anwendungen werden von den Softwareherstellern protokolliert, insbesondere bei der Eingabe, Änderung und Löschung von Daten.
Die Softwarearchitektur stellt Berechtigungskonzepte mit Nutzerrollen zur Verfügung. Der Auftraggeber kann seinen Mitarbeitern ("Sekundärnutzern") den Zugang zur Software gewähren, um im Auftrag des Auftraggebers tätig zu sein. Die Berechtigungen der Sekundärnutzer schließen die Möglichkeit der Einrichtung weiterer Sekundärnutzer aus. Der Auftraggeber ist für die Verwaltung der Berechtigungen der Sekundärnutzer selbst verantwortlich. Alle Nutzer melden sich mit individuellen Zugangsdaten (Benutzername, Passwort) in der Software an. Zugriffe auf die Software werden protokolliert, insbesondere bei der Eingabe, Änderung und Löschung von Daten. Diese Sicherheitsmaßnahmen gewährleisten den angemessenen Schutz der personenbezogenen Daten und werden im Rahmen dieses Vertrags umgesetzt.

4. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.
Beschreibung des Trennungskontrollvorgangs:
Da aktuell keine angestellten Mitarbeiter vorhanden sind, ist das gesamte Berechtigungskonzept ausschließlich auf Galina Spedt (Auftragnehmer) ausgelegt. Eine Trennung von der Software des Kunden erfolgt entweder durch ein offlinearbeitendes Praxis-/Krankenhausinformationssystem vor Ort oder einen geschützten Onlinezugriff am „remote"-Arbeitsplatz getrennt von der Onlineeingabe in das Meldeportal der Landeskrebsregisters über den firmeneigenen Laptop. Der Onlinezugriff erfolgt durch zwei getrennte Bereiche/Logins.

D. Maßnahmen zur Sicherung der Integrität

1. Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt, werden:
Beschreibung der Datenintegrität:
Personenbezogene Daten werden in dem IT-System der Praxis/Klinik vor Fehlfunktionen geschützt. In den Landeskrebsregistern obliegt dieser Schutz vor Fehlfunktionen der internen IT-Struktur.

2. Übertragungskontrolle

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:
Beschreibung der Übertragungskontrolle:
Der Zugang zu den Praxis-/Klinikinformationensystem ist sowohl personenbezogenen nachvollziehbar durch Einloggen mit eigenem Profil oder erfolgt über einen zentralen Zugang für alle Mitarbeiter.
Die Login-Verwaltung wird in der Praxis/Klinik von dem verantwortlichen Arzt/Ärztin oder IT-Support an den Auftragnehmer weitergegeben. In der Praxis/Klinik werden zentrale Ansprechpartner bestimmt. Beiden Parteien liegen die Login-Daten vor und können jederzeit verwendet werden.
Die personenbezogenen Daten werden ausschließlich auf dem elektronischen Weg an die Landeskrebsregister übertragen. Es sind keine physikalischen Datentransfers vorgesehen. Jegliche Weitergabe von personenbezogenen Daten, die im Auftrag des Auftraggebers erfolgt, darf nur in dem Umfang erfolgen, der zuvor mit dem Auftraggeber abgestimmt wurde. Die Übertragung der Daten erfolgt ausschließlich über vollständig verschlüsselte Verbindungen an den zertifizierten Server. Es sind keine anderen Datenübertragungswege zugelassen.

3. Transportkontrolle

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:
Beschreibung der Transportkontrolle:
Eine Datenübertragung findet von dem Praxis-/Krankenhausinformationssystem Datenextraktionssoftware „tumorscout" von Galina Spedt als Auftragnehmer in Meldeportale der Landeskrebsregister statt. Es finden keine dokumentarischen Zwischenschritte bzw.

Abspeicherungen/Transporte in ein anderes Dokumentationsmanagementsystem statt. Die Dokumentation erfolgt vor Ort in den Räumen des Auftraggebers oder am „remote“-Arbeitsplatz in blickgeschützten Arbeitsräumen. Papierunterlagen sind nicht vorhanden. Die Sperrung der Arbeits-Hardware ist beim Verlassen des Arbeitsplatzes obligat. Telefongespräche finden in einem geschützten Raum statt.

4. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.
Beschreibung des Eingabekontrollvorgangs:
Der Zugriff auf die Praxis-/Krankenhausinformationssysteme erfolgt ausschließlich zum Lesen in der digitalen Akte. Eine Veränderung der Daten erfolgt nicht. Die Zugriffsdaten zum System werden vom Auftraggeber an die Auftragnehmerin für die Durchführung der Auftragsdatenverarbeitung weitergegeben. Die Zugangsdaten zum Meldeportal der Landeskrebsregisters werden vom Auftraggeber an den Auftragnehmer weitergegeben. Der Auftraggeber bleibt für das Landeskrebsregister der ärztliche Ansprechpartner, der Auftragnehmer der dokumentarische Ansprechpartner. Ab Vertragsbeginn werden sämtliche Meldungen vom Auftragnehmer durchgeführt.

E. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
Eine regelmäßige Datensicherung der Festplatte findet statt. Diese wird feuer- und zugriffssicher im Safe aufbewahrt.

2. Rasche Widerherstellbarkeit

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten
und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.
Beschreibung der Maßnahmen zur raschen Widerherstellbarkeit: Die Widerherstellbarkeit der Daten auf der Hardware erfolgt über die Datensicherung. Die Widerherstellbarkeit im Praxis-/Krankenhausinformationssystem trägt der Auftraggeber. Die Widerherstellbarkeit der erfolgten Meldungen an die Landeskrebsregister tragen
Krebsregister selbst bzw. die auftragende Behörde.

3. Zuverlässigkeit

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:
Beschreibung der Maßnahmen zur Zuverlässigkeit:
Datenwiederherstellung durch die Datensicherung der Arbeits-Hardware ist möglich. Für Fehlfunktionen im Praxis-/Krankenhausinformationssystem trägt der Auftraggeber die Verantwortung. Für Fehlfunktionen im Meldeportal der Landeskrebsregister trägt das Krebsregister selbst bzw. die auftragende Behörde die Verantwortung.

F. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

1. Überprüfungsverfahren

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

Beschreibung der Überprüfungsverfahren:
Eine Überprüfung des Datenschutzes wird durchgeführt.

2. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:
Beschreibung der Maßnahmen zur Auftragskontrolle:
Weisungen des Auftraggebers werden dokumentiert. Vereinbarungen, welche Daten zu welchem Zwecke verarbeitet werden, sind in dem geschlossenen Vertrag festgehalten.

Anlage 2

Unterauftragsverhältnisse

Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den folgenden weiteren Auftragsverarbeitern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt.
Die Unternehmen sind nachfolgend genannt:

Auftragnehmer	**Auftragnehmer Funktion/Tätigkeit:**
Tumorscout GmbH Am Zirkus 4 10117 Berlin	Medizinische Dokumentation, Datenerfassungstool Softwareentwicklung, Betrieb und Wartung Von Tumorscout
Litixsoft GmbH Karl-Tauschnitz-Str. 8 04107 Leipzig	„Tumorscout“ Softwareentwicklung, Betrieb und Wartung Von Tumorscout
axaris – software & systeme GmbH Max-Eyth-Weg 2 89160 Dornstadt	„extraxx“- Datenextraktionssoftware
TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen	Fernwartungstool zur Kommunikation zwischen Auftraggeber und Auftragnehmer
WatchGuard Technologies Wendenstrasse 379 20537 Hamburg	IT-Sicherheitsdienste, VPN-Anbindung
Frau Galina Spedt „onkodata“ In der Schlei 33 56357 Buch	Tumordokumentation

Anlage 3

Verpflichtung zur Wahrung der Vertraulichkeit, von Geschäftsgeheimnissen und zur Beachtung des Datenschutzes sowie ggf. zur Wahrung von Berufsgeheimnissen

Im Rahmen der beauftragten Tätigkeit entsteht Kontakt mit personenbezogenen Daten. Ich verpflichte mich hiermit zur Beachtung des Datenschutzes, insbesondere zur Wahrung der Vertraulichkeit. Die Verpflichtung besteht umfassend. Die personenbezogenen Daten dürfen nicht ohne Befugnis verarbeitet werden, darüber hinaus dürfen diese anderen Personen nicht unbefugt mitgeteilt oder zugänglich gemacht werden. Insbesondere besteht die Verpflichtung, die datenschutzrechtlichen Vorgaben und Weisungen im Unternehmen zu beachten.
Unter einer Verarbeitung versteht die EU-Datenschutz-Grundverordnung (DSGVO) jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
„Personenbezogene Daten“ im Sinne der DSGVO sind alle Informationen, die sich auf einen identifizierten oder identifizierbaren Menschen beziehen; als identifizierbar wird ein Mensch angesehen, der direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck seiner physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.
Unter Geltung der DSGVO können Verstöße gegen Datenschutzbestimmungen nach § 42 BDSG (Bundesdatenschutzgesetz) sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden. Datenschutzverstöße können zugleich eine Verletzung arbeits- oder dienstrechtlicher Pflichten bedeuten und entsprechende Konsequenzen haben. Datenschutzverstöße sind ebenfalls mit möglicherweise sehr hohen Bußgeldern für das Unternehmen bedroht, die gegebenenfalls zu Ersatzansprüchen Ihnen gegenüber führen können.

Verpflichtung zur Wahrung von Geschäftsgeheimnissen
Über Angelegenheiten des Unternehmens, die beispielsweise Einzelheiten des Unternehmens betreffen, sowie über Geschäftsvorgänge und Zahlen des internen Rechnungswesens und alle als Geschäftsgeheimnisse zu definierenden Vorgänge nach § 2 Nr. 1 Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), ist – auch nach Beendigung des Beschäftigungsverhältnisses – Verschwiegenheit zu wahren, sofern sie nicht öffentlich bekannt geworden sind. Hierunter fallen auch Vorgänge von Drittunternehmen, mit denen man dienstlich befasst ist. Alle dienstlichen Tätigkeiten betreffenden Aufzeichnungen, Abschriften, Geschäftsunterlagen, Ablichtungen, dienstlicher oder geschäftlicher Vorgänge, die für die Tätigkeit überlassen oder von Auftragnehmerin angefertigt werden, sind vor Einsichtnahme Unbefugter zu schützen. Die Verletzungen dieser führen mit sich eine Strafbarkeit, insbesondere nach § 23 GeschGehG.

Hinweise für Berufsgeheimnisträger
Unabhängig von der vorgenannten datenschutzrechtlichen Verpflichtung ist über im Rahmen der Berufsausübung anvertrauten Informationen strikte Verschwiegenheit zu wahren. Dies gilt ebenfalls für Zeugenaussagen in Zivil-, Straf- oder Verwaltungsprozessen. Verstöße gegen diese Verschwiegenheitspflicht sind nach § 203 StGB strafbar.
Die Verpflichtung zur Verschwiegenheit besteht ohne zeitliche Begrenzung und auch nach Beendigung der Tätigkeit fort.

Ort, Datum Unterschrift des Verantwortlichen

Ort, Datum Unterschrift des Verpflichteten