RABER

Gerhart-Hauptmann-Straße 6

99096 Erfurt

Telefon: (0361) 43 05 63 7

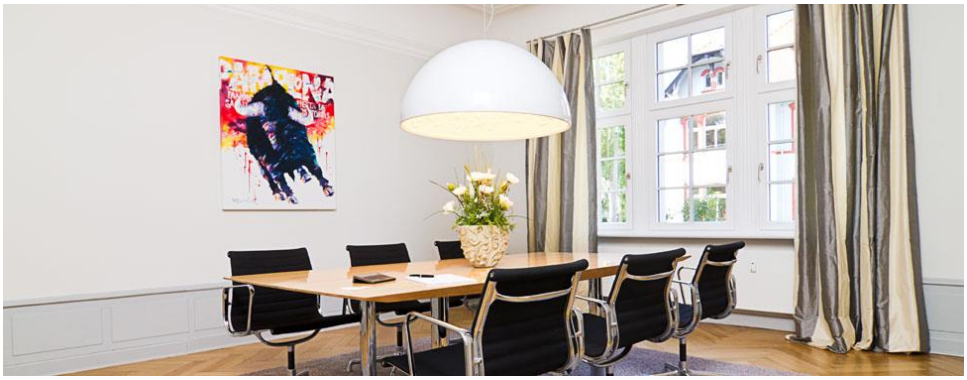
E-Mail: recht@raberundcoll.de

Telefax: (0361) 43 05 63 99

In Kooperation mit:

UTE GAJEWSKY
STEUERBERATERIN

INFO-Post 1/2018



EU-Datenschutzgrundverordnung

Was ändert sich am 25.05.2018?

Rechtsanwalt Manfred Raber

Fachanwalt für Bau- und Architektenrecht

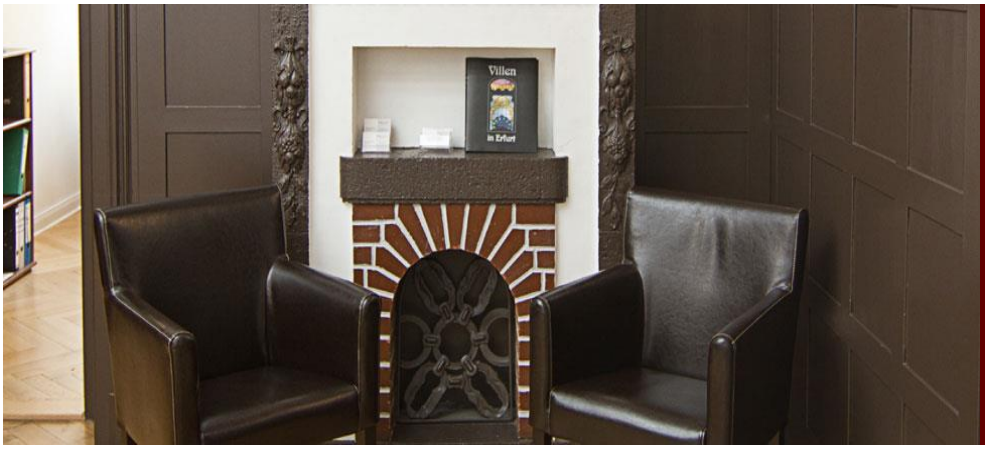
Fachanwalt für Arbeitsrecht

Bauherren Schutz Bund e.V.

arge baurecht im DeutschenAnwaltVerein

Mitglied im AnwaltVerein

QUALITÄT DURCH FORTBILDUNG



Gliederung

Einleitung

Am 25 Mai 2018 tritt die neue EU-Datenschutzgrundverordnung (EU-DSGVO) in Kraft.

Betroffen von der Verordnung sind alle, die automatisiert personenbezogene Daten verarbeiten, insbesondere Personalakten elektronisch verwalten oder Kundendateien führen.

In erheblichem Umfang betroffen sind Fördergesellschaften und Förderbanken, Wohnungsunternehmen, Makler und Verwalter, medizinische Dienstleister, Rechtsanwälte, Steuerberater und Notare aber auch jeder Handwerksbetrieb und sogar der Sportverein mit seiner elektronischen Mitgliederverwaltung.

Wegschauen hilft nicht, denn die Konsequenzen wären fatal.

Zum einen drohen Bußgelder in Höhe von bis zu 20 Mio € oder bis zu 4 % des weltweiten Jahresumsatzes eines Unternehmens.

Zum anderen und dies ist sehr zeitnah zu erwarten, droht eine Abmahnwelle, die sich wahrscheinlich in erster Linie gegen kleine und mittelständische Unternehmen richten wird, die sich vielfach auf die neue Rechtslage nicht vorbereiten.

1. Was ist neu?

Die neue Verordnung regelt die Rechtsgrundlagen der Datenverarbeitung, die Rechte der Betroffenen und die Pflichten der Verantwortlichen.

Diese treffen Informationspflichten gegenüber Betroffenen.

Erstmalig gibt es einen Anspruch der Betroffenen auf Löschung personenbezogener Daten („Recht auf Vergessenwerden").

Verbunden ist all dies mit Anforderungen, die an den Datenschutz in einem Unternehmen gestellt werden.

Hierzu gehört der technische und organisatorische Datenschutz einerseits, ein Verzeichnis der Verarbeitungstätigkeiten, eine Datenschutzfolgenabschätzung und vieles mehr.

2. Wann dürfen Daten verarbeitet werden?

Daten dürfen Sie verarbeiten, wenn eine der folgenden Voraussetzungen gegeben ist:

- der Betroffene, der mindestens 16 Jahre alt ist, hat **eingewilligt**
- die Datenverarbeitung ist für die **Vertragserfüllung** erforderlich
- die Datenverarbeitung ist für die Durchführung **vorvertraglicher** Maßnahmen erforderlich
- die Datenverarbeitung ist zur Erfüllung **sonstiger rechtlicher Pflichten** erforderlich
- die Datenverarbeitung erfolgt zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten, wobei schutzwürdige Interessen des Betroffenen nicht überwiegen dürfen.

Damit geht die DSGVO nicht über die bisherige gesetzliche Regelung hinaus.

Jedes Unternehmen, jeder Vermieter, jeder Arzt, Steuerberater, Notar und jeder Handwerker beschränkt seine Datenverarbeitung auf das, was für die Erfüllung der vertraglichen Pflichten gegenüber dem Kunden, Mieter, Patienten oder Mandanten erforderlich ist.

Abgedeckt ist auch die Datenverarbeitung bei Personen, die noch keine Kunden sind, z. B. Mietinteressenten, denn dort geht es um die Erfassung von Daten zur Durchführung vorvertraglicher Maßnahmen.

Die Datenerfassung als solche ist also regelmäßig nicht das Problem, vielmehr Art und Umfang der Daten.

Ich empfehle daher dringend, unabhängig von der Rechtfertigung der Datenverarbeitung zur Erfüllung vertraglicher oder vorvertraglicher Verpflichtungen, die Einwilligung des Betroffenen einzuholen.

Bei Vermietern sollte dies bereits beim ersten Kontakt mit den Mietinteressenten durch Hinweis auf einen Mieterfassungsbogen erfolgen, den der Mietinteressent unterschreibt, spätestens dann mit der Unterschrift unter dem Mietvertrag.

Makler und Hausverwalter sollten eine entsprechende Textpassage in Ihre Vertragsformulare aufnehmen, soweit noch nicht geschehen.

Gleiches gilt für Dienstleister, die die Einwilligung des Betroffenen in die Mandatsübernahmebedingungen aufnehmen.

Für die Mehrzahl der Unternehmen, insbesondere die Handwerksbetriebe empfiehlt sich ein ausdrücklicher Hinweis in der Auftragsbestätigung, verbunden mit der Aufforderung an den Kunden, bei fehlendem Einverständnis zu widersprechen.

3. Gibt es Daten, die nicht verarbeitet werden dürfen?

Ja, diese Daten gibt es.

Es sind dies alle Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, ebenso wie die Verarbeitung von genetischen Daten, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung.

Alle Daten, die Tatbestände betreffen, welche eine Ungleichbehandlung verbieten, also im AGG abgebildet sind, dürfen selbstverständlich nicht verarbeitet werden.

Diese Daten spielen für ein Unternehmen, gleich ob Handwerksbetrieb, Wohnungsunternehmen oder Dienstleister ohnehin keine Rolle, sieht man von einigen wenigen Ausnahmen ab.

Ärzte und Krankenhäuser kommen zwangsläufig nicht umhin, Gesundheitsdaten aufzunehmen und zu speichern.

Aus diesem Grund gibt es Ausnahmetatbestände, damit dort, wo es erforderlich ist, abweichend vom grundsätzlichen Verarbeitungsverbot, sensible Daten verarbeitet werden dürfen, was sich in der Mehrzahl der Fälle allerdings auf Gesundheitsdaten beschränken dürfte.

4. Rechte der Betroffenen

a) Informationspflichten

Kernstück der DSGVO sind die umfangreichen Rechte von Betroffenen, verbunden mit entsprechenden Pflichten der Verantwortlichen.

Der Pflichtenkatalog zeigt zugleich, worauf sich Unternehmen vorbereiten müssen, wenn sie die Realisierung von Bußgeldern oder erfolgreichen Abmahnangegriffen aus dem Wege gehen wollen.

Folgende Informationen müssen nämlich auf Wunsch des Betroffenen oder dessen (anwaltlichen) Vertreter mitgeteilt werden

- Name und Kontaktdaten dessen, der die Daten verarbeitet (Verantwortlicher)
- soweit es einen Datenschutzbeauftragten gibt, auch dessen Kontaktdaten
- Zweck und Rechtsgrundlage der Datenverarbeitung
- bei Weitergabe der Daten, Angaben zum Empfänger
- Dauer der Datenspeicherung
- Belehrungen des Betroffenen über seine Rechte auf Auskunft, Berichtigung, Löschung, Datenportabilität, Widerspruchsrecht und Beschwerderecht zur Aufsichtsbehörde.

Dabei kann der Betroffene nicht nur Auskunft verlangen, sondern auch die Übermittlung seiner, beim Verantwortlichen gespeicherten personenbezogenen Daten.

Mit den neuen Informations-/Auskunftsrechten können betroffene Personen also Auskunft darüber verlangen, welche Daten gespeichert sind, woher diese stammen, an wen sie übermittelt werden, zu welchem Zweck die Datenverarbeitung erfolgt, etwa zur Erstellung eines Profilings, und wie lange sie gespeichert werden.

Es ist nicht auszuschließen, dass es in Unternehmen, die in erheblichem Umfang Daten speichern, zukünftig massenhaft zur Geltendmachung von Auskunftsrechten kommen wird.

Für die Mehrzahl der hier angesprochenen Unternehmen, die zum größten Teil auch in persönlichen Kontakt zum Kunden stehen, dürfte dies nicht der Fall sein.

b) Datenportabilität

Neu ist das Recht auf Datenübertragung, wonach der Betroffene ein datenverarbeitendes Unternehmen anweisen kann, bei Wechsel des Anbieters die Daten zu übertragen.

Für die Mehrzahl der Unternehmen, sei es Dienstleister oder Handwerksbetriebe ist dies nicht von Bedeutung.

c) Recht auf Vergessen werden

Sind Daten erst einmal erhoben, erfreuen sie sich einer beträchtlichen Langlebigkeit, der Betroffene steht dem hilflos gegenüber.

Die DSGVO gibt dem Betroffenen nunmehr ein Recht auf Löschung seiner Daten.

Voraussetzung dieses Löschungsrechts ist, dass

- die Speicherung der Daten nicht mehr notwendig ist
- der Betroffene seine Einwilligung widerrufen hat
- die Daten zu Unrecht verarbeitet werden

oder

- eine Rechtspflicht nach nationalem oder EU-Recht besteht.

Wer Daten im Rahmen dessen, was zulässig ist erhebt, wird vom Löschungsanspruch regelmäßig nur insoweit betroffen sein, als ein Widerruf des Betroffenen vorliegt oder die Speicherung der Daten schlicht nicht mehr notwendig ist.

Klar und eindeutig ist die Rechtslage, wenn der Betroffene seine Einwilligung widerrufen hat.

Weniger klar ist, wann die Speicherung der Daten nicht mehr notwendig sein soll.

Bedeutet der Abschluss eines Mandats des Steuerberaters oder Rechtsanwaltes die Löschungspflicht?

Soll der Handwerksbetrieb nach Abnahme und Zahlung der Schlussrechnung den Kunden löschen oder besteht die Löschungspflicht nach Ablauf der Gewährleistungsfrist?

Abgesehen davon, dass der Kundenstamm und damit zwangsläufig die Kundendaten entscheidend den Unternehmenswert beeinflusst, ist dies schon rein praktisch gar nicht denkbar, denn sonst müssten bei jedem neuen Auftrag die Kundendaten komplett neu angelegt werden.

Als gesichert gilt jedoch, dass personenbezogene Daten von Mietinteressenten, mit denen kein Mietvertrag zustande gekommen ist, nicht gesammelt und gespeichert werden dürfen, sondern zu löschen sind.

Gleiches gilt, wenn der Mietvertrag beendet ist, also nach Auszug des Mieters, wenn alle gegenseitigen Ansprüche erledigt sind.

Was für einen Vermieter also relativ klar ist, stellt sich für den Steuerberater komplett anders dar, denn er betreut seine Mandanten über viele Jahre.

Im Zweifelsfall ist es daher zu empfehlen, generell eine Einverständniserklärung des Kunden einzuholen, dass dessen Daten über den konkreten Vertrag hinaus gespeichert werden.

Konsequenterweise sieht die DSGVO neben dem Recht auf Löschung auch ein Recht auf Berichtigung vor.

Dies ist eigentlich eine Selbstverständlichkeit, zumal auch der Verantwortliche der Datenverarbeitung ein Interesse an Speicherung richtiger Daten haben sollte.

5. Was muss ich in meinem Unternehmen beachten?

a) TOM

Nach der DSGVO müssen Verantwortliche geeignete technische und organisatorische Maßnahmen (TOM) treffen, um Datenschutz und Datensicherheit zu gewährleisten.

Das klingt gut, lässt allerdings viele Fragen offen.

Welche Anforderungen stellt die DSGVO an die Datensicherheit in einem Handwerksbetrieb, wenn nicht einmal der Server des Bundestages vor Hackerangriffen sicher ist?

Welche Maßnahmen konkret erforderlich sind, hängt letztlich vom Stand der Technik sowie davon ab, wie wahrscheinlich es ist, dass sich Risiken realisieren.

Insofern wird man unterschiedliche Anforderungen an Unternehmen stellen müssen, deren Datenverarbeitung sich auf die Mitarbeiter sowie die Vertragsabwicklung beschränkt.

Weit höhere Anforderungen ergeben sich naturgemäß bei der Speicherung sensibler Daten, wie es bei Förderbanken/Fördergesellschaften, Ärzten, aber auch Rechtsanwälten und Steuerberatern der Fall ist.

Auch Wohnungsunternehmen, die Daten über die Vermögensverhältnisse Ihrer Mietinteressenten oder Mieter einholen, begründen Risiken, die entsprechende Anforderungen an die Datensicherheit bedingen.

Besonders hoch sind die Anforderungen naturgemäß dort, wo die Datenverarbeitung selbst im Mittelpunkt der unternehmerischen Tätigkeit steht.

In der Praxis wird sicherlich kaum jemals der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) den Server des Trockenbaubetriebs prüfen.

Relevant werden die Fälle allerdings dann, wenn es zu Pannen kommt und diese entweder durch Betroffene angezeigt oder durch das Unternehmen pflichtgemäß gemeldet werden.

Dann spätestens entscheidet die von der Aufsichtsbehörde vorgefundene tatsächliche Datensicherung darüber, ob und wie hoch das Bußgeld ausfällt.

Die Pflicht zur Einhaltung hoher Standards der Datensicherheit sollte also nicht auf die leichte Schulter genommen werden.

b) Verzeichnis der Verarbeitungstätigkeiten

Die DSGVO schreibt vor, dass der Verantwortliche, welcher Daten verarbeitet, selbst oder ein durch ihn beauftragter Auftragsverarbeiter verpflichtet ist, ein Verzeichnis der Verarbeitungstätigkeiten zu führen.

Dies ist in Betrieben ab 250 Mitarbeiter immer der Fall, im Übrigen dann, wenn

- die Datenverarbeitung ein Risiko für die Rechte und Freiheiten betroffener Personen birgt
- die Datenverarbeitung nicht nur gelegentlich erfolgt
- lediglich die Verarbeitung besonderer Datenkategorien erfolgt.

Derzeit ist unklar, ob die Regelung wörtlich zu verstehen ist, denn ein Risiko besteht immer, sodass nach dem Wortlaut streng genommen auch alle kleine Unternehmen unter 250 Mitarbeiter ein Verzeichnis der Verarbeitungstätigkeiten erstellen müssten.

Hätte der Verordnungsgeber jedoch gewollt, dass alle Unternehmen unter die Verpflichtung zur Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten fallen, so hätte es keines Limits von 250 Arbeitnehmern bedurft.

Man wird danach folgendes sagen können.

Ausgenommen sind Unternehmen mit weniger als 250 Mitarbeiter, wenn

- die Datenverarbeitung nicht die Haupttätigkeit, sondern Nebentätigkeit im Rahmen der Erbringung der eigentlichen Haupttätigkeit ist
- ein gesteigertes Risiko bei der Datenverarbeitung nicht gegeben ist.

Allerdings wäre es wünschenswert, wenn die Aufsichtsbehörden eine Klarstellung vornehmen würden.

Bisher ist dies nicht erfolgt.

Wer daher absolut sichergehen möchte, wird auch mit weniger als 250 Mitarbeitern ein Verzeichnis der Verarbeitungstätigkeiten in Schrift- oder Textform erstellen.

Dieses Verzeichnis sollten Sie in der bis zum 24.05.2018 verbleibenden Zeit am besten durch Ihren zukünftigen Datenschutzbeauftragten erarbeiten lassen.

Verlangt wird eine Dokumentation und Übersicht aller Verfahren, bei denen personenbezogene Daten verarbeitet werden.

Bei jedem Unternehmen ist dies zunächst die Verarbeitung der Arbeitnehmerdaten, gegebenenfalls auch der Daten der Nachunternehmer und Lieferanten, schließlich der Kunden.

Dabei lassen sich unterschiedliche Phasen voneinander unterscheiden.

Das Wohnungsunternehmen nimmt erstmals personenbezogene Daten bei der Erfassung des Mietinteressenten auf und übernimmt diese nach Abschluss des Mietvertrages in die Mieter-Datei.

Diese Daten verändern sich während des Mietverhältnisses; in jedem Fall kommen neue Daten hinzu.

Dabei handelt es sich auch um sensible Daten, wie beispielsweise die Erklärung des Vorvermieters, die Drittschuldnererklärung bei Forderungspfändungen oder das Vermögensverzeichnis im Falle der Vollstreckung.

Es empfiehlt sich daher frühzeitig mit der Erstellung eines Verzeichnisses aller denkbaren Verfahren bei personenbezogenen Daten zu beginnen, aus dem sich außerdem Name und Kontaktdaten des Datenschutzbeauftragten im Unternehmen, die Löschfristen und der eingehaltene technische und organisatorische Datenschutz ergeben.

Einsichtsberechtigt in das Verzeichnis ist die Aufsichtsbehörde.

c) Datenschutzfolgenabschätzung

Immer dann, wenn ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht, muss der Verantwortliche eine Datenschutzfolgenabschätzung nach der DSGVO vornehmen.

Auch hier kommt es letztlich auf den Einzelfall an.

Die Speicherung personenbezogener Daten wie Name, Vorname, Geburtsdatum und Geschlecht sowie Adresse eines Mitglieds im Sportverein dürfte kaum mit einem hohen Risiko für die Rechte und Freiheiten des Betroffenen verbunden sein.

Anders kann es sein, wenn es um die Speicherung von Daten eines Patienten oder eines Mandanten sowie eines Fördermittelberechtigten geht.

Im Zweifelsfall sollte daher jeder Verantwortliche eine Datenschutzfolgenabschätzung vornehmen.

Bestehen hierfür Anhaltspunkte, so stellt sich die Frage, ob die vorgesehenen Sicherheitsvorkehrungen ausreichen, um den Schutz der Daten zu gewährleisten.

Hierzu sollte der Datenschutz vor Angriffen Dritter durch ein Fachunternehmen geprüft und durch entsprechende Software verbessert werden.

Damit dürfte die Mehrzahl der Unternehmen ihrer Verpflichtung nach Abschätzung und Abwendung des Datenschutzfolgenrisikos im ausreichenden Umfang nachgekommen sein.

Wenn auch das nicht reicht, muss freilich die Aufsichtsbehörde konsultiert werden.

Wenden Sie sich in diesem Fall an den Thüringer Landesbeauftragten für den Datenschutz und Informationsfreiheit.

Was Sie in jedem Fall beachten sollten, ist, dass die Datenschutzfolgenabschätzung schriftlich dokumentiert wird.

Verknüpften Sie am besten die Datenschutzfolgenabschätzung mit dem ohnehin durch Sie zu erstellenden Verzeichnis der Verarbeitungstätigkeiten.

Wer vom Bau ist, der weiß – Wer schreibt der bleibt.

d) Was ist im Falle einer Datenpanne zu beachten?

Kommt es zu einer Verletzung des Schutzes personenbezogener Daten, also zu einer Datenpanne, so muss diese innerhalb von 72 Stunden nach Bekanntwerden der Verletzung der Aufsichtsbehörde gemeldet werden.

Inhalt der Meldung ist

- Beschreibung des Vorfalls, Angabe der betroffenen Daten und der betroffenen Personen
- Name und Kontaktdaten des Datenschutzbeauftragten
- Beschreibung der Folgen der Datenschutzverletzung
- Beschreibung der bereits ergriffenen oder vorgesehenen Maßnahmen zur Behebung oder Abmilderung der Verletzung

Ansprechpartner ist der Bundesbeauftragte für den Datenschutz.

Daneben müssen Sie außerdem die Betroffenen grundsätzlich ebenfalls benachrichtigen.

e) Datenschutzbeauftragter

Nach der DSGVO müssen Unternehmen einen betrieblichen Datenschutzbeauftragten benennen, wenn im Unternehmen in der Regel mindestens zehn Personen ständig mit der Datenverarbeitung beschäftigt sind.

Dies ergibt sich nicht aus der DSGVO, sondern aus § 38 DSAnpUG-EU.

Relevant ist also nicht die Anzahl der Personen im Unternehmen, sondern die Anzahl der Personen, die mit Datenverarbeitung beschäftigt sind.

Unabhängig von der Anzahl der Personen, die mit der Datenverarbeitung beschäftigt sind, müssen auch solche Unternehmen einen betrieblichen Datenschutzbeauftragten benennen, die der Datenschutzfolgenabschätzung unterliegen.

Dies betrifft sicherlich in erheblichem Umfang Steuerberater, Notare und Rechtsanwälte, ganz besonders jedoch Ärzte und die durch sie verarbeiteten Gesundheitsdaten.

Es ist nicht damit getan, zur Wahrung des äußeren Anscheins einer/einem Mitarbeiterin/Mitarbeiter den Titel des Datenschutzbeauftragten zu übertragen.

Der Datenschutzbeauftragte muss entsprechend fachlich qualifiziert sein, weshalb er sich ständig fortbilden muss.

In keinem Fall sollte zum Datenschutzbeauftragten bestimmt werden, wer auf der Abschussliste steht, denn der Datenschutzbeauftragte genießt besonderen Kündigungsschutz.

Wenn Sie sicher gehen wollen, beauftragen Sie einen externen Datenschutzbeauftragten.

Worin bestehen die Aufgaben des Datenschutzbeauftragten?

- Er berät den Verantwortlichen.
- Er überwacht die Einhaltung des DSGV und anderer Rechtsquellen des Datenschutzrechts.
- Er schult Mitarbeiter, die mit Datenverarbeitung beschäftigt sind.
- Er berät im Zusammenhang mit der Datenschutzfolgenabschätzung und deren Überwachung.
- Er arbeitet mit der Aufsichtsbehörde zusammen, für die er zugleich Ansprechpartner ist.

Fazit:

In den verbleibenden Wochen bis zum 24.05.2018 sollten Sie prüfen, ob und in welchem Umfang Sie Daten über Mitarbeiter und Kunden erheben.

Sie sollten dafür sorgen, dass Ihnen die entsprechenden Einwilligungen der Betroffenen vorliegen.

Achten Sie darauf, dass Sie nur solche Daten erheben, die wirklich erforderlich und vom Datenschutz gedeckt sind.

Sorgen Sie dafür, dass Daten, die nicht notwendig sind, gelöscht werden.

Erstellen Sie ein Verzeichnis der Verarbeitungstätigkeiten und prüfen Sie, ob die von Ihnen erhobenen Daten sensibel sind und damit eine Datenschutzfolgenabschätzung erforderlich machen.

Wenn Sie mehr als zehn Mitarbeiter mit Datenverarbeitung beschäftigen oder sensible Daten, wie Gesundheitsdaten verwalten, benennen Sie frühzeitig einen Datenschutzbeauftragten.

Sollten Sie sich entscheiden einen Mitarbeiter mit dieser Aufgabe zu betrauen, so sollten Sie nicht lange warten, diesen auf eine Schulung zu schicken.

Erfurt, 09.04.2018

Manfred Raber Rechtsanwalt
Fachanwalt für Arbeitsrecht
Fachanwalt für Bau- und Architektenrecht