KANZLEI AM STEINMARKT
Kuchenreuter, Dr. Stangl, Alt • Rechtsanwälte PartGmbB

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

Rundschreiben 03/2018

Thema: Europäische Datenschutzgrundverordnung – Herausforderung für Unternehmen und Vereine – / Datenschutzrecht

1. Einleitung

Datenschutz wird zunehmend zu einem der wichtigsten Bereiche unternehmerischer Tätigkeit. Nicht erst seit dem „Facebook-Skandal" ist die Frage des Umgangs mit persönlichen Daten in der öffentlichen Wahrnehmung zu einem beherrschenden Thema geworden.

Zum 25.05.2018 tritt – ohne Übergangsfristen! – ein einheitliches europäisches Datenschutzrecht in Kraft. Es handelt sich um unmittelbar wirksames europäisches Recht, welches in der „Datenschutzgrundverordnung (DS-GVO)" enthalten ist.

Vieles, was in der Neuregelung enthalten ist, war schon bisher geltendes Recht, die neue Verordnung bringt trotz allem aber eine Vielzahl von Konkretisierungen und neuen Regelungen.

Da die Aufsichtsbehörden Verstöße gegen die Verordnung mit drastischen Geldbußen belegen können – die europäische Verordnung sieht eine Größenordnung von bis zu 20 Mio. Euro oder bis zu 4 % des Weltjahresumsatzes vor – bedarf es einer intensiven Befassung mit der Materie. Auch wenn im Regelfall wohl Geldbußen in derart drastischer Höhe nicht verhängt werden, so ist doch damit zu rechnen, dass zumindest offenkundige oder schwerwiegende Verstöße mit empfindlichen Geldbußen geahndet werden können.

Die nachfolgende Abhandlung soll einen groben Überblick über die neuen Regelungen geben. Erfahrungen aus der Praxis existieren noch nicht. Von daher ist natürlich vieles noch unsicher, manche Details werden wohl erst im Rahmen der praktischen Umsetzung und letztendlich auch im Rahmen der Ahndung von möglichen Verstößen konkretisiert werden. Trotz allem sollten sich die Verantwortlichen bis zum in Kraft treten der neuen Regelungen damit befassen.

Verantwortlich im Sinne des Gesetzes sind natürlich grundsätzlich Firmeninhaber und Unternehmensleitungen sowie die für die Datenverarbeitung im Unternehmen Verantwortlichen. Nicht außer Acht gelassen kann jedoch werden, dass etliche Bestimmungen nicht nur für die Datenverarbeitung im Geschäftsverkehr Anwendung finden, sondern beispielsweise auch auf die Datenverarbeitung und Datenspeicherung in Vereinen oder ähnlichen Organisationen. Auch dieser Problemkreis muss sich also mit den Themen beschäftigen.

2. Grundsätzliche Überlegungen

Die DS-GVO gilt für weite Bereiche, sie gilt sowohl für die vollständige oder teilweise automatisierte Verarbeitung personenbezogener Daten, als auch für die nicht automatisierte Verarbeitung solcher Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Eine elektronische Datenverarbeitung kann auch lediglich aus einem Computer bestehen, selbst ein nach bestimmten Kriterien geordnetes Dateisystem in „Papierform" (beispielsweise eine Mitgliederdatei eines Vereins) kann hierunter fallen.

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

Als personenbezogene Daten werden alle Informationen bezeichnet, die sich auf eine bestimmte natürliche Person beziehen, die Person muss identifiziert oder identifizierbar sein, beispielsweise durch ein Nummernsystem, durch Namen, Adressen oder persönliche Merkmale. Hierzu gehören beispielsweise auch Mitgliedsnummern, Religionszugehörigkeit, Geschlecht, etc.

Unter den Begriff der Datenverarbeitung fällt jeglicher Umgang mit solchen Daten, sowohl das Erheben, Speichern, Ändern, Nutzen, als auch das Übermitteln, Verknüpfen oder Löschen der Daten. Jeglicher Umgang mit persönlichen Daten stellt ein Verarbeiten dar.

Ausgenommen vom Geltungsbereich der DS-GVO sind eigentlich nur rein private / familiäre Datensammlungen.

In allen Fällen, in denen die DS-GVO Anwendung finden kann, müssen sich die jeweiligen Verantwortlichen, sei es die Unternehmensleitung oder der Vereinsvorstand, über die Konsequenzen im Klaren sein. Letztendlich ist Datenschutz „Chefsache" – die drastischen Geldbußen Treffen im Zweifel die Unternehmensleitung oder das Unternehmen an sich –, weshalb es erforderlich ist, sich einen Gesamtüberblick zu verschaffen, in welchen Bereichen Umgang mit persönlichen Daten erfolgt, inwieweit dieser Umgang gehandhabt wird und zu dokumentieren ist, inwieweit Außenstehende in die Datenverarbeitung einbezogen sind und wie der Umgang mit diesen vertraglich geregelt ist, weiter auch, wie mit den nach der DS-GVO bestehenden Rechten der von der Verarbeitung betroffenen Personen umzugehen ist. Die grundsätzliche Frage, die sich jeder stellen muss, ist natürlich auch, ob die Verarbeitung der Daten überhaupt nachweisbar zulässig ist. Geregelt muss auch werden, wie mit „Pannen" umzugehen ist, und wie im Zweifel der Kontakt mit den Aufsichtsbehörden zu halten ist.

Nicht zuletzt ist auch zu klären, inwieweit ein Datenschutzbeauftragter zu bestellen ist.

Verantwortlich hierfür sind alle Personen (sowohl natürliche Personen als auch juristische Personen), die mit personenbezogenen Daten von anderen umgehen. Es kann hier sowohl eine bestimmte Person persönlich verantwortlich sein, als auch eine Organisation bzw. deren Organe.

3. Verzeichnis von Verarbeitungstätigkeiten

Die DS-GVO fordert, dass die Verantwortlichen ein Verzeichnis über alle Verarbeitungstätigkeiten zu führen haben, die in ihrem Unternehmen oder in ihrem Verein durchgeführt werden. Erforderlich ist die Dokumentation wo, wie und in welchem Zusammenhang mit personenbezogenen Daten gearbeitet wird. In ein solches Verzeichnis sind beispielsweise sämtliche EDV-Programme aufzunehmen, welche auf gespeicherte Daten von Betroffenen Zugriff nehmen, um beispielsweise Korrespondenz zu adressieren, eMails zu versenden, Bankgeschäfte zu erledigen, Beiträge einzuziehen, Werbung zu verbreiten, usw.

Die Erstellung eines solchen Verzeichnisses ist Pflicht. Lediglich in wenigen Ausnahmefällen besteht diese Verpflichtung nicht. Theoretisch gibt es die Verpflichtung zwar nicht für Unternehmen mit weniger als 250 Mitarbeitern, allerdings nur dann, wenn die Datenverarbeitung nur gelegentlich erfolgt und keine besonderen Datenkategorien, wie Gesundheits- oder Religionsdaten verarbeitet werden.

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

Es reicht also schon aus, wenn beispielsweise die Daten der Mitarbeiter inkl. der Religionszugehörigkeit (Abführung der Kirchensteuer!) gespeichert sind, um die Ausnahme hinfällig zu machen. Wenn der Unternehmens- oder Vereinszweck nur aufgrund der Datenspeicherung erfüllt werden kann (beispielsweise die Mitgliederdateien des Vereins regelmäßig gepflegt werden, um die Vereinsmitglieder informieren und Beiträge einziehen zu können), liegt nicht nur eine „nur gelegentliche" Datenverarbeitung vor. In der Praxis werden die Fälle, in welchen ein Verzeichnis nicht erstellt werden muss, wohl die Ausnahme bleiben.

Es handelt sich bei dem zu erstellenden Verzeichnis allerdings um ein betriebsinternes Verzeichnis. Dieses Verzeichnis muss Dritten (mit Ausnahme der Aufsichtsbehörden) nicht offengelegt werden. Eine besondere Bedeutung hat das Verzeichnis insbesondere im Hinblick darauf, dass mit diesem Verzeichnis auch die Nachweispflichten gegenüber der Aufsichtsbehörde erfüllt werden können.

Eine bestimmte Form ist nicht vorgesehen, abgesehen davon, dass das Verzeichnis (nahezu selbstredend) in deutscher Sprache aufzustellen ist. Die Aufstellung kann sowohl schriftlich, als auch in Dateiform erfolgen.

Allerdings muss das Verzeichnis regelmäßig auf dem neuesten Stand gehalten werden. Aus Gründen der Dokumentation ist es empfehlenswert, Änderungen jeweils auch für sich gesehen zu dokumentieren, um zu vermeiden, dass nach einer Änderung die frühere Fassung des Verzeichnisses nicht mehr verfügbar ist.

Der Mindestinhalt des Verarbeitungsverzeichnisses besteht aus folgenden Angaben:

- Name und Kontaktdaten des oder der Verantwortlichen
- Zweck der Verarbeitung
- Beschreibung der betroffenen Personenkreise und der betroffenen Datenkategorien
- Beschreibung der möglichen Empfängerkreise der Daten, insbesondere auch soweit Daten in Drittstaaten gelangen können oder müssen
- soweit Löschfristen vorgesehen sind, Angabe der Löschfristen

Über den Mindestinhalt hinaus kann das Verzeichnis auch weitere Angaben umfassen. Wenn das Verzeichnis auch betriebsintern dazu dienen soll, sich einen Überblick über die Datenverarbeitungstätigkeiten im Betrieb zu verschaffen, ist es sinnvoll, im Verzeichnis auch die konkrete Art der Verarbeitung zu dokumentieren (Datenerhebung, Speicherung, Datenabfrage, usw.), darüber hinaus die für die Datenverarbeitung bestehenden Rechtsgrundlagen.

Vor allem letzteres ist von Bedeutung, da für jede Art von Datenverarbeitung eine Rechtsgrundlage existieren muss (Details im nächsten Kapitel). Auf entsprechende Anforderung der Aufsichtsbehörden muss auch die Rechtmäßigkeit der Datenverarbeitung dargelegt werden.

4. Rechtsgrundlagen für die Datenverarbeitung

Grundsätzlich ist das Datenschutzrecht ein restriktives Recht. Der Umgang, insbesondere die Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten, wenn die Datenverarbeitung nicht ausdrücklich durch eine Rechtsgrundlage gedeckt ist.

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

Die in der Praxis problemloseste Rechtsgrundlage ist natürlich die Einwilligung der betroffenen Person.

Soweit der Betroffene freiwillig darin eingewilligt hat, dass seine persönlichen Daten in einem bestimmten Umfang bzw. für einen bestimmten Zweck von einem bestimmten Adressaten verarbeitet werden, ist die Datenverarbeitung zulässig.

Auch in den Fällen, in denen eine Einwilligung des Betroffenen nicht vorliegt, kann die Datenverarbeitung zulässig sein. Insbesondere ist die Verarbeitung personenbezogener Daten zulässig, wenn die Verarbeitung für die Erfüllung eines Vertrages oder einer sonstigen rechtlichen Verpflichtung erforderlich ist, darüber hinaus ist die Verarbeitung auch dann zulässig, wenn es für die Wahrung den berechtigten Interessen des die Daten verarbeitenden oder eines Dritten erforderlich ist und die Interessen des von der Verarbeitung Betroffenen nicht die Interessen des Verarbeitenden überwiegen.

Aus dieser Formulierung ergibt sich bereits, dass letztendlich bei der Verarbeitung von Daten immer dann, wenn nicht eine ausdrückliche Einwilligung vorliegt, eine Interessenabwägung notwendig ist. Derjenige, der die Daten verarbeitet, muss also immer abwägen, ob die Erfüllung des Zwecks der Datenverarbeitung auch unter Berücksichtigung der Interessen des Betroffenen an der Nichtverarbeitung der Daten zulässig ist.

Diese Abwägung umgeht natürlich, wer über eine Einwilligung zur Verarbeitung der Daten verfügt.

Eine wirksame Einwilligung setzt allerdings voraus, dass sie

- freiwillig,
- für einen bestimmten Zweck,
- nach klarer und verständlicher Information des Betroffenen über die Umstände der Datenverarbeitung und das Recht, die Einwilligung zu widerrufen,
- durch eine eindeutige Handlung

erfolgt ist. Vor allem die eindeutige Einwilligungshandlung ist manchmal problematisch, es reicht nicht aus, dass beispielsweise bei einer Datenerhebung über das Internet das Feld mit der „Einwilligung zur Datenverarbeitung" bereits vorab angekreuzt ist und vom Betroffenen das entsprechende Kreuz entfernt werden muss (so genannte „Opt-out-Lösung"), es ist vielmehr die aktive Zustimmung (also das aktive Ankreuzen des entsprechenden Kästchens) erforderlich.

Die Einwilligung muss durch den die Datenverarbeitenden jederzeit nachgewiesen werden können. Sie muss also entsprechend dokumentiert sein. Darüber hinaus kann der Betroffene die Einwilligung auch jederzeit widerrufen.

Liegt eine Einwilligung nicht vor, so muss einer der anderen bereits oben erwähnten Gründe für die Verarbeitung der Daten vorliegen.

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

Weitgehend klar ist als Rechtsgrundlage der Datenverarbeitung die Erfüllung eines Vertrages. Im Rahmen einer Vertragserfüllung ist es zumindest erforderlich, die Personalien der Vertragsparteien (Namen, Adressen, sonstige Kontaktdaten) zu verarbeiten. Hierzu können je nach Eigenart des Vertrages auch sonstige Daten, wie z. B. Daten über die Zahlungsfähigkeit, gehören.

Sind die Daten nicht zur Vertragserfüllung erforderlich, kann die Wahrung berechtigter Interessen des für die Datenverarbeitung Verantwortlichen ebenfalls eine Rechtsgrundlage darstellen.

Der Begriff der „Wahrung berechtigter Interessen" ist sehr weit gefasst. Hierunter fällt beispielsweise die Speicherung von Daten von Verfahrensbeteiligten durch Rechtsanwälte, hierunter können auch unter bestimmten Fällen die Datenverarbeitung für Werbezwecke und Marktforschung, aber auch die Auswertung von Kundendaten fallen. Erforderlich ist aber auch hier immer eine Interessenabwägung.

Unabhängig davon, auf welcher Rechtsgrundlage die Datenverarbeitung beruht, ist auch die berechtigte Verarbeitung von Daten an bestimmte Voraussetzungen gebunden.

Zum einen dürfen die Daten nur für den Zweck verarbeitet werden, für den sie erhoben wurden. Beispielsweise ist die Weitergabe von Daten, die im Zusammenhang mit einem bestimmten Vertrag erhoben werden, für Werbezwecke außerhalb der Vertragszwecke nicht zulässig, wenn dieser nicht ausdrücklich zugestimmt wurde.

Darüber hinaus müssen die Daten natürlich richtig sein. Es muss vor allem sichergestellt werden, dass die Daten aktuell gehalten werden, umgekehrt muss für den Betroffenen die Möglichkeit gegeben sein, ohne unzumutbaren Aufwand zu veranlassen, dass seine Daten bei Änderungen der Verhältnisse auch angepasst werden (also beispielsweise Adressänderungen, Namensänderungen infolge Heirat oder ähnliches).

Eine längerfristige Speicherung der Daten muss im Übrigen erforderlich sein. Insbesondere, wenn für das konkret bestehende Verhältnis zwischen dem Betroffenen und dem Datenverwender nicht mehr existiert und auch keine sonstigen Pflichten mehr bestehen, die Daten zu speichern (diese Verpflichtungen können sich beispielsweise aus Aufbewahrungsvorschriften im Steuerrecht oder anderen Regelungen ergeben), müssen die Daten gelöscht werden oder zumindest soweit anonymisiert werden, dass eine individuelle Zuordnung nicht mehr möglich ist.

Von besonderer Bedeutung ist, dass die Einhaltung der genannten Vorschriften nicht nur im Innenverhältnis erforderlich ist, sondern von den Verantwortlichen auch dokumentiert und in bestimmten Fällen nachgewiesen werden muss.

Bei dieser Dokumentationspflicht handelt es sich um eine Verpflichtung, die die zuständigen Aufsichtsbehörden relativ leicht überprüfen können. Hier müssen die Behörden eigentlich nur verlangen, dass die entsprechenden Unterlagen zur Dokumentation vorgelegt werden. Es kann also damit gerechnet werden, dass die Behörden vor allem auf diesen Gesichtspunkt einen Schwerpunkt ihrer Kontrolltätigkeiten legen werden, da hier relativ einfach die schriftlich dokumentierte Einhaltung der Vorschriften kontrolliert werden kann.

Von daher ist dringend zu empfehlen, dass die Einhaltung dieser Vorschriften (durch das oben bereits beschriebene Verfahrensverzeichnis) klar dokumentiert wird.

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

Ebenso zu dokumentieren ist im Übrigen auch, dass nicht nur die jeweils für den Datenschutz Verantwortlichen ihren Verpflichtungen nachkommen, sondern dass alle die mit persönlichen Daten in Berührung kommen, auf die Einhaltung der Vorschriften verpflichtet werden.

5. Verarbeitung von Daten durch Dritte

Wenn Daten im Auftrag eines Anderen verarbeitet werden, liegt eine so genannte Auftragsverarbeitung vor. Dies betrifft nicht nur die direkte Verwendung der Daten (beispielsweise die Überlassung von Kundendaten an ein Call-Center, die Überlassung der Buchhaltung an ein externes Buchhaltungsbüro oder den Steuerberater), sondern auch Tätigkeiten, die mit einem Zugriff auf gespeicherte Daten als „Nebeneffekt" verbunden sind. Hierzu gehört beispielsweise der IT-Dienstleister, der die EDV-Anlage eines Unternehmens wartet und im Rahmen seiner Wartungsarbeiten naturgemäß auch die Möglichkeit hat, auf die auf dieser EDV-Anlage gespeicherte Daten zuzugreifen.

Für die Auftragsverarbeitung gelten gesonderte Regelungen.

Je nachdem, welche Tätigkeiten im Rahmen einer „externen Auftragsverarbeitung" ausgeführt werden, kann unter bestimmten Voraussetzungen die Einwilligung der betroffenen Personen zur Datenweitergabe erforderlich sein. Dies ist allerdings nicht immer der Fall. Wenn der Auftragsverarbeiter lediglich genau definierte Tätigkeiten weisungsgebunden ausübt (beispielsweise die Buchhaltung des Unternehmens extern erledigt wird), ist eine ausdrückliche Einwilligung oder sonstige gesetzliche Grundlage nicht erforderlich. Handelt es sich allerdings um eine Datenweitergabe zur Erbringung externer Leistungen, wie Kundenbetreuung, Inkassotätigkeit mit Forderungsübertragung, etc., bedarf es möglicherweise einer Einwilligung.

Jedenfalls besteht die Verpflichtung, einen Auftragsverarbeiter sorgfältig auszuwählen, insbesondere unter Berücksichtigung der Frage, ob dieser die datenschutzrechtlich einwandfreie Auftragsdurchführung gewährleisten kann. Darüber hinaus ist eine vertragliche Vereinbarung erforderlich, die insbesondere die gesamten Vertragsumstände genau definiert und die die notwendige Verpflichtung zur Vertraulichkeit und Einhaltung der datenschutzrechtlichen Vorschriften enthält. Auch der Verbleib der Daten bei Beendigung des Auftragsverhältnisses ist zu regeln. Der Auftraggeber muss sich in diesen Fällen auch Kontrollrechte einräumen lassen, um sicherzustellen, dass er die Erfüllung seiner Verpflichtungen durch den mit der Verarbeitung beauftragten Dritten kontrollieren kann. Hierzu gehört auch die Erforderlichkeit, sich Zutrittsrechte zu den Betriebsräumen zu verschaffen. Dies ist vor allem dann von Bedeutung, wenn beispielsweise freiberuflich tätige Dritte in ihrer Privatwohnung arbeiten. In diesem Fall steht einem Betretungsrecht zunächst das Recht an der eigenen Wohnung entgegen, so dass man sich entsprechende Betretungsrechte ausdrücklich zusichern lassen muss, um die Kontrolle im Rahmen des Vertragsverhältnisses sicherzustellen. Zu regeln ist auch das Vorgehen bei Beendigung des Vertragsverhältnisses, insbesondere auf welchem Weg eine Rückgabe der Daten oder eine Löschung sichergestellt werden kann.

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

6. Sicherheitsmaßnahmen bei der Datenverarbeitung

Eine Kernanforderung bei jeglicher Verarbeitung von Daten ist die (technische) Realisierung von Sicherheitsmaßnahmen. Inzwischen dürfte auch dem letzten Verwender von EDV-Techniken klar sein, dass die Nutzung der elektronischen Datenverarbeitung mit vielfältigen Problemen und Risiken verbunden ist. Cyber-Angriffe, Pishing-Versuche, Hacker – eine Vielzahl von Schlagworten kennzeichnet die Bedrohungen der elektronischen Datenverarbeitung. Durch entsprechende Sicherheitslücken können fahrlässig oder auch aufgrund vorsätzlich begangener Straftaten eine Vielzahl von teils äußerst sensiblen Daten in falsche Hände geraten.

Durch entsprechende Sicherheitsmaßnahmen muss sichergestellt werden, dass die Daten vertraulich bleiben, also geschützt sind, die Integrität der Daten, also die Unversehrtheit der Informationen sichergestellt ist und die Daten auch jederzeit verfügbar sind, also nicht durch Pannen, Fehler oder Eingriffe Dritter die Zugriffsmöglichkeit auf die Daten beeinträchtigt ist.

Zur Sicherstellung der technischen Voraussetzungen für den sicheren Datenumgang bedarf es eines ausreichenden technischen Sachverstandes. Die Zeiten, in denen ein „interessierter Laie" in der Lage ist, mit einfachen Mitteln kleines Netzwerk in einem kleineren Unternehmen ohne Inanspruchnahme entsprechender Spezialisten sicher zu betreiben, dürften weitgehend vorbei sein. Zu groß sind inzwischen die technischen Anforderungen und auch die Risiken.

Um die notwendige Datensicherheit zu gewährleisten, bedarf es einerseits einer Vielzahl von organisatorischen Maßnahmen, andererseits aber auch technischer Vorrichtungen und technischer Vorsorge, für die entsprechender Sachverstand in Anspruch genommen werden sollte. Derartiger Sachverstand ist zwar nicht „umsonst" zu haben, die Kosten hierfür liegen aber weit unter den Kosten, die durch Pannen in diesem Bereich verursacht werden können.

Betriebsintern muss sichergestellt werden, dass nur die Personen Zugriff auf Daten haben, die den Zugriff auch benötigen. Dies kann durch Vergabe von unterschiedlichen Benutzerrechten geschehen, durch Sperren des Zugangs zu bestimmten Bereichen der EDV etc. Wichtig ist auch, an ausscheidende Mitarbeiter zu denken, um sicherzustellen, dass diese z. B. nicht über noch vorhandene Passwörter Zugang zu sensiblen Daten erhalten können.

Erforderlich ist auch eine genaue Analyse der möglichen Risiken, die durch fahrlässig begangene Fehler, vorsätzliche Eingriffe von außen oder auch durch technische Probleme (Systemabstürze) oder Einflüsse von außen (bspw. Brand – oder Wasserschäden) entstehen können. Für alle diese Risiken bedarf es einer entsprechenden Risikoanalyse und der Entwicklung von Abwehrmaßnahmen.

Zur Sicherstellung der technischen Sicherheit der Datenverarbeitung gehört auch der Einsatz von Verschlüsselungstechnologien, soweit diese erhältlich sind und soweit diese auch in der täglichen Handhabung praktikabel sind. Auch hier bedarf es einer fachkundigen Betreuung, vor allem auch dann, wenn es darum geht, dass auf die EDV-Anlage eines Unternehmens von außen zugegriffen werden soll (z. B. wenn Mitarbeiter von zu Hause oder vom Mobilgerät aus arbeiten und auf die Server zugreifen). Hier ist auf jeden Fall darauf zu achten, dass die technischen Sicherheitsmaßnahmen einen unbefugten Zugriff Dritter verhindern. Nicht unproblematisch ist in diesem Zusammenhang die Nutzung eigener (privater) Geräte der Mitarbeiter.

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

Zur Gewährleistung der Sicherheitsmaßnahmen gehört im Übrigen auch, dass die Systeme auf dem neuesten Stand gehalten werden und vor allem Sicherheitsupdates und Ergänzungen regelmäßig auf dem neuesten Stand gehalten werden.

Ein besonderes Augenmerk sollte man im Übrigen auch auf die E-Mail-Korrespondenz legen. Vor allem bei der Versendung an eine größere Anzahl von Adressaten muss darauf geachtet werden, dass nicht sämtliche Adressdaten aller E-Mail-Empfänger für alle Adressaten der E-Mail erkennbar sind („Bcc" – Versand). Besonders muss natürlich auch darauf geachtet werden, dass E-Mails nicht falsch adressiert werden.

Unverzichtbar ist natürlich auch das Vorhalten entsprechender Virenschutzsoftware, von Firewalls und ähnlichem. Die beste Firewall nützt aber nichts, wenn sicherheitsrelevante Bereiche (EDV-Arbeitsplätze, Serverräume und ähnliches) ohne besondere Sicherungsmaßnahmen betreten werden können und sich Unbefugte auf diesem Weg Zugriff „am Gerät" verschaffen können.

Zur Datensicherheit gehört auch eine Absicherung gegen Datenverluste aller Art (sei es durch Eingriffe Dritter oder auch nur durch technische Defekte). Unverzichtbar ist also auch eine regelmäßige Datensicherung, wobei es empfehlenswert ist, die Sicherung so zu organisieren, dass auch bei größeren Unglücksfällen – man denke an einen Brand in den Betriebsräumen – nicht sämtliche Daten verloren sind, z. B. durch räumlich getrennte Verwahrung von Sicherheitskopien.

7. Datenschutzbeautragter

Besonders heikel könnte die Verpflichtung in der neuen DS-GVO sein, einen Datenschutzbeauftragten zu benennen. Zweck des Datenschutzbeauftragten ist die Selbstkontrolle des Unternehmens im gesamten Benbereich des Datenschutzes.

Ob ein Datenschutzbeauftragter bestellt werden muss bestimmt sich nach verschiedenen Gesichtspunkten.

Erforderlich ist ein Datenschutzbeauftragter auf jeden Fall dann, wenn mindestens 10 Personen im Unternehmen mit der automatisierten Datenverarbeitung befasst sind.

Auch Betriebe, die diese Personenzahl nicht erreichen, müssen einen Datenschutzbeauftragten bestellen wenn sie bestimmte besonders sensible Daten verarbeiten wie z.B. Gesundheitsdaten, genetische Daten, Daten über rassische oder ethnische Herkunft, politische Einstellung, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit oder Straftaten. Gehört die Verarbeitung derartiger Daten zum Kernbereich des Unternehmens, ist ein Datenschutzbeauftragter auch bei kleineren Unternehmen erforderlich. Ein Datenschutzbeauftragter ist im Übrigen auch erforderlich, wenn zur Tätigkeit des Unternehmens gehört, Personen regelmäßig und systematisch zu überwachen.

In den meisten Fällen wird ein Datenschutzbeauftragter schon deswegen erforderlich sein, weil mehr als 10 Personen mit der Datenverarbeitung befasst sind. Es ist unbedeutend, ob es sich um Vollzeit- oder Teilzeitkräfte handelt oder ob es sich bspw. in einem Verein um ehrenamtlich Tätige handelt. Es zählt nur die Zahl der Personen. Auch wenn die Zahl von 10 Personen nicht erreicht wird, muss bei Verarbeitung bestimmter Daten ein Datenschutzbeauftragter bestellt werden.

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

Dies ist z.B. der Fall, wenn in einem Unternehmen aus dem Bereich der Gesundheitssorge Daten verarbeitet werden, die für den Unternehmenszweck erforderlich sind (also bspw. Daten von Patienten bzw. Kunden). Anders ist dies nur dann, wenn die sensiblen Daten lediglich aufgrund einer gesetzlichen Verpflichtung gespeichert werden ohne das es für die betriebliche Tätigkeit darauf ankommen würde (wenn bspw. die Daten der Religionszugehörigkeit der Mitarbeiter für Zwecke der Lohnbuchhaltung gespeichert werden).

Auch wenn ein Datenschutzbeauftragter nicht zwingend erforderlich ist, kann er freiwillig benannt werden. In Betracht kommt sowohl ein interner Datenschutzbeauftragter, also ein eigener Mitarbeiter des Unternehmens, als auch ein externer Dienstleister. Sofern ein eigener Mitarbeiter benannt werden soll, darf dies dann allerdings nicht in Konflikt mit seiner sonstigen Tätigkeit kommen. Wohl nicht in Betracht als Datenschutzbeauftragter kommt z.B. ein Mitarbeiter, der für die EVD-Anlage des Unternehmens verantwortlich ist.
Zur Person des Datenschutzbeauftragten ist zumindest derzeit noch streitig, ob Datenschutzbeauftragter auch ein (Mit-) Inhaber des Betriebes sein kann. Diese Frage ist zumindest derzeit noch nicht abschließend geklärt.

Die Benennung muss zwar nicht schriftlich erfolgen, sollte aber dokumentiert sein. Sinnvoll ist also auf jeden Fall den Datenschutzbeauftragten schriftlich zu benennen.

Der Aufgabenbereich des Datenschutzbeauftragten ist vielfältig. Er sollte Verantwortliche und die Mitarbeiter des Betriebes hinsichtlich ihrer Pflichten informieren, die Einhaltung der gesetzlichen Vorschriften überwachen, beraten, als Anlaufstelle für die Aufsichtsbehörde dienen und mit dieser zusammen arbeiten und betroffene Personen bei Datenschutzverstößen beraten. Er ist allerdings nicht verantwortlich für die Umsetzung der Datenschutzvorschriften, verantwortlich bleibt die Geschäftsleitung bzw. die Verantwortlichen.

Die Person des Datenschutzbeauftragten ist der Aufsichtsbehörde mitzuteilen. Die Kontaktdaten sind im Übrigen auch zu veröffentlichen. Der Datenschutzbeauftragte ist zwar nicht persönlich zu benennen, allerdings ist zumindest dessen Kontaktadresse bspw. die E-Mail-Adresse zu benennen. Zu beachten ist, dass, wenn der Datenschutzbeauftragte über eine E-Mail-Adresse zu erreichen ist, die Eingänge unter dessen E-Mail-Adresse nur von diesem selbst oder seinem Vertreter gelesen werden können.

Grundsätzlich ist zur Problematik des Datenschutzbeauftragten anzumerken, dass die Überprüfung, ob ein Datenschutzbeauftragter erforderlich ist und ob ein solcher bestellt ist, für die Aufsichtsbehörden sehr einfach zu bewerkstelligen ist. Dies erleichtert den Behörden natürlich die Aufgabe, umso mehr ist zu erwarten, dass die Überprüfung, ob ein Datenschutzbeauftragter bestellt ist, von den Behörden gründlich vorgenommen wird und ggf. auch sanktioniert wird. Von daher sollte jeder Betrieb auf jeden Fall bis zum Inkrafttreten der Regelung am 25.05.2018 überprüfen, ob ein Datenschutzbeauftragter bestellt werden muss und ggf. einen Datenschutzbeauftragten bestellen.
Dieser muss natürlich für seine Tätigkeit grundsätzlich geeignet sein, es ist allerdings viel schwieriger zu überprüfen, ob eine Person für die Aufgabe als Datenschutzbeauftragter geeignet ist, als zu überprüfen, ob ein Datenschutzbeauftragter überhaupt existiert. Im Zweifel ist es daher besser, eine nicht optimal geeignete Person als Datenschutzbeauftragten zu benennen als gar keinen Datenschutzbeauftragten zu bestellen. Letzteres kann von den Aufsichtsbehörden dann mit Sicherheit sanktioniert werden.

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

8. Rechte von Personen die von der Datenverarbeitung betroffen sind

Die neue DS-GVO verpflichtet Unternehmen und Vereine, die Datenverarbeitung betreiben, zur Wahrung von verschiedenen Rechten der von der Datenverarbeitung betroffenen Personen.

Zunächst besteht die Verpflichtung, die von der Datenverarbeitung betroffenen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu informieren, was zu welchem Zweck mit personenbezogenen Daten geschieht.

Zu informieren ist insbesondere über:

- Namen und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten, soweit ein solcher bestellt ist
- Zwecke für die die Daten verarbeitet werden
- Rechtsgrundlagen der Datenverarbeitung bzw. Interessen des die Daten Verarbeitenden, wenn die Daten aufgrund einer Interessensabwägung verarbeitet werden
- mögliche Empfänger der Daten, wenn diese weitergegeben werden sollen
- Dauer der Speicherung der Daten bzw. Kriterien einer Datenlöschung
- Hinweise auf Auskunfts-, Berichtigungs- und Löschungsrechte
- Hinweise auf die Möglichkeit eine erteilte Einwilligung jederzeit ohne Begründung zu widerrufen
- Hinweis auf das Beschwerderecht bei der Aufsichtsbehörde

Auch bisher schon stand den Betroffenen ein Recht auf Auskunft zu. Der Verarbeiter muss eine Auskunft lediglich erteilen, wenn der Betroffene dies beantragt. Dem Betroffenen muss auf seinen Antrag hin mitgeteilt werden, welche Daten über ihn gespeichert sind bzw. er muss auch darüber informiert werden, dass keine Daten gespeichert sind, wenn dies nicht der Fall ist. Das Auskunftsrecht umfasst das Recht auf Erteilung einer Auskunft darüber welche Daten zu der Person insgesamt erfasst sind, zu welchem Zweck diese verarbeitet werden, welche Daten verarbeitet werden, an wen diese weitergegeben werden und wie lange diese voraussichtlich gespeichert werden und ein Hinweis auf die weiteren betroffenen Rechte und die Beschwerdemöglichkeiten. Die Auskunft ist konkret anhand der Daten des jeweils Auskunftsersuchenden zu erteilen und darf nicht lediglich allgemein erteilt werden. Auskunft ist im Übrigen kostenlos zu erteilen.

Soweit die Daten fehlerhaft sind, hat der Betroffenen einen Anspruch auf Berichtigung der Daten.

Ein Anspruch auf Löschung besteht, wenn die weitere Speicherung nicht mehr erforderlich ist und es insbesondere hierfür keine Rechtsgrundlage gibt. Auch von Haus aus unrechtmäßig erhobene und gespeicherte Daten sind zu löschen. Soweit Streitigkeiten über die Richtigkeit der Daten bestehen, darf der für die Verarbeitung Verantwortliche die Daten zwar noch speichern, aber nicht mehr verarbeiten, also bspw. Dritten übermitteln.

Sowohl eine Berichtigung als auch eine Löschung sind den Berechtigten nachzuweisen. Bei einer Berichtigung kann dies durch Übermittlung der aktualisierten Daten geschehen, bei der Löschung reicht es aus, dass verbindlich mitgeteilt wird, dass die Daten gelöscht sind.

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

Neu ist im Übrigen auch ein Recht auf Datenübertragbarkeit. Soweit ein Betroffener personenbezogene Daten an einen Verwender übermittelt hat, hat er einen Anspruch darauf, dass er diese in einem gängigen Dateiformat zur Verfügung gestellt bekommt oder diese an einen anderen weitergeleitet werden. Dies gilt aber nur für die Daten, die der Betroffene selbst übermittelt hat.

Betroffene können darüber hinaus der Verarbeitung ihrer Daten widersprechen. Allerdings muss er plausible Gründe dafür nennen weshalb er der Verarbeitung widerspricht, wenn die Datenverarbeitung auf einer Interessenabwägung zwischen den Interessen des Verwenders und des Betroffenen beruht. Wenn der Betroffene hier neue Gesichtspunkte vorbringt, muss der die Daten Verarbeitende eine erneute Interessenabwägung vornehmen, ob die Datenverarbeitung (weiterhin) gerechtfertigt ist.

Widerspricht der Betroffene allerdings der Verwendung von Daten für Werbemaßnahmen, so bedarf es hierfür keiner Gründe. Wird Werbemaßnahmen widersprochen, dürfen die Daten nicht mehr hierfür verwendet werden.

Vor allem die Vielzahl von möglichen Betroffenen führt letztendlich dazu, dass es erforderlich ist, sich mit diesen Rechten individuell auseinanderzusetzen und auch sich damit auseinanderzusetzen wie auf die Geltendmachung dieser Rechte reagiert werden soll.

9. Datenschutzverletzungen

Großen Wert legt die gesetzliche Neuregelung auf Verhaltensvorgaben, wenn es zu einer „Verletzung des Schutzes personenbezogener Daten" kommt. Eine solche Verletzung liegt immer dann vor, wenn die gewünschte Datensicherheit beeinträchtig ist. Unbedeutend ist, ob diese Verletzung versehentlich oder bewusst erfolgt ist. Es bedarf hier also keines bewussten Verstoßes. In Betracht kommt neben einer unbefugten Offenlegung oder unbefugtem Zugang auch Datenverlust oder Datenveränderung. Auch nur denkbar negative Konsequenzen sind ausreichend, es ist nicht erforderlich, dass es zu irgendeinem nachweisbaren Schaden der betroffenen Person kommt. Neben der möglichen Vernichtung der Daten (also z.B. einer Löschung) betrifft die Regelung auch den Verlust der Daten, wenn also die Daten nicht mehr zugängig sind (bspw. bei Diebstahl eines Datenträgers oder ähnlichem).

Bei einem unbefugten Zugriff auf die Daten reicht schon die Möglichkeit des unbefugten Zugriffs. Es muss sich also noch nicht einmal ein unbefugter Zugriff ereignet haben.

Bei allen Fällen der Verletzung des Datenschutzes besteht die Pflicht diese unverzüglich der Aufsichtsbehörde zu melden. Nur dann wenn die Verletzung voraussichtlich nicht zu einem Risiko für Rechte und Freiheiten der betroffenen Personen führt, entfällt die Meldepflicht. Dies ist allerdings sicherlich nur in Ausnahmefällen der Fall. Denkbar wäre hier z.B. der Fall, dass irgendwelche Daten zerstört werden, die sowieso schon längst hätten gelöscht sein müssen und damit unwiederbringlich verloren sind.

Die Meldepflicht besteht, sobald der Verstoß bekannt ist, wobei dafür Sorge getragen werden muss, dass Verstöße den Verantwortlichen mitgeteilt werden.

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

Die Meldung hat „unverzüglich" zu erfolgen. Es darf im Zweifel nicht damit zugewartet werden, bis alle Einzelheiten eines möglichen Verstoßes bekannt und aufgeklärt sind, insbesondere, wenn mit einer Zeitverzögerung zusätzliche Risiken verbunden sind. Schon wenn die ersten Informationen vorliegen, besteht die Meldepflicht, ggf. besteht dann die Pflicht Details zum Sachverhalt noch nach zu melden, wenn diese bekannt werden.

Das Gesetz geht davon aus, dass „unverzüglich" einem Zeitraum von max. 72 Stunden entspricht. Dieser Zeitraum wird wohl auch nur in Ausnahmefällen überschritten werden dürfen, wenn dies besonders begründet werden kann.

Verstöße gegen die Verpflichtungen sind mit hohen Geldbußen bedroht.

Darüber hinaus besteht die Verpflichtung, betroffene Personen zu benachrichtigen. Diese Verpflichtung besteht allerdings nur dann, wenn „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten" der betroffenen Person besteht.

Ob dieses Risiko besteht, ist jeweils im Einzelfall abzuwägen. Hierbei kann natürlich auch berücksichtigt werden, dass evtl. abhanden gekommene Daten besonders gesichert sind – bspw. durch Verschlüsselung – und ein Zugang nicht ohne weiteres möglich ist. Es setzt aber natürlich dann auch voraus, dass entsprechende Sicherungsmaßnahmen auch frühzeitig getätigt wurden.

Besonders die Verständigung betroffener Personen kann natürlich auch Risiken mit sich bringen. Die Frage, ob eine Benachrichtigung notwendig ist, muss daher im Einzelfall konkret und sorgfältig abgewogen werden. Wird die Person benachrichtigt, besteht natürlich das Risiko, dass diese ihrerseits Schadensersatz- oder Haftungsansprüche gelten macht – berechtigterweise oder auch unberechtigt –. In diesem Fall empfiehlt sich auf jeden Fall eine gründliche Überlegung und ggf. auch Beratung.

Ist die Benachrichtigung erforderlich, so ist die betroffene Person unter Angabe des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners darüber zu informieren, welche Verletzung sich ereignet hat, welche Folgen diese wahrscheinlich oder möglicherweise für den Betroffenen hat und ein Hinweis darauf, welche Maßnahmen zur Vermeidung von Nachteilen und negativen Folgen ergriffen wurden bzw. welche Maßnahmen dem Betroffenen empfohlen werden, um einen Schaden zu vermeiden.

10. Mögliche Folgen von Verstößen

Verstöße gegen die Datenschutzvorschriften bringen finanzielle Risiken in verschiedener Hinsicht mit sich. Zum einen können die Aufsichtsbehörden Geldbußen in erheblicher Höhe verhängen. Die in der Verordnung genannten Beträge erreichen astronomische Höhen. Auch wenn diese Beträge sicherlich in dieser Höhe nicht bei alltäglichen Verstößen verhängt werden, so ist doch damit zu rechnen, dass schon allein die Höhe der maximal angedrohten Geldbußen dazu führt, dass im Zweifel die Behörden auch für leichtere Verstöße schon sehr schmerzhafte Geldbußen verhängen. Die Verordnung sieht ausdrücklich vor, dass die Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein sollen.

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

Ob sich bei der Höhe der Geldbußen gegenüber der bisherigen Praxis – auch bis jetzt waren Verstöße gegen Datenschutzvorschriften ja mit Bußgeldern bedroht – Änderungen ergeben, wird man abwarten müssen. Zu vermuten ist aber, dass die Zahl der Verstöße, bei denen Bußgelder verhängt werden, steigen werden.

Als weiteres nicht zu unterschätzendes Risiko kommt auch die Verpflichtung zum Schadenersatz hinzu. Ist einem Betroffenen ein Schaden entstanden, so hat er Anspruch auf Schadensersatz. Dies kann zum einen Anspruch auf Ersatz tatsächlich entstandener materieller, also in Geld direkt zu bemessender Schäden, sein. Zu denken ist aber auch an sog. „immaterielle Schadensersatzansprüche", die den Anspruch auf Schmerzensgeld nach sich ziehen können. Hier wird man natürlich abwarten müssen wie die Praxis, insbesondere die in diesem Fall dann zuständigen Zivilgerichte, Verstöße bewerten werden und in welcher Höhe sie im Zweifel Schmerzensgelder zusprechen werden, wenn ein Betroffener geltend macht er sei durch einen Datenschutzverstoß in seinen Persönlichkeitsrechten verletzt worden. Auch hier kann es durchaus um Forderungen in beträchtlicher Höhe gehen.

Nicht zuletzt können auch Mitbewerbe möglich offenkundige Verstöße als Wettbewerbswidriges Verhalten abmahnen.

Wie sich die Ahndungspraxis in der Zukunft entwickelt, lässt sich momentan nur schwer vorher sehen. Die Befugnisse der Aufsichtsbehörden gehen nach den gesetzlichen Neuregelungen sehr weit. In welchem Umfang und mit welcher Intensität die Behörden dann letztendlich ihren Verpflichtungen nachkommen, wird sicherlich auch davon abhängig sein, wie sich die personelle und materielle Ausstattung der Behörden in der Zukunft darstellt. Man sollte allerdings nicht darauf spekulieren, dass die Behörden den Verstößen sowieso nicht nachgehen werden, da sie dazu nicht gerüstet sind. Auch wenn vielleicht in der ersten Zeit die Kontroll- und Ahndungspraxis nicht zu intensiv ausfällt, besteht immer die Gefahr, dass aufgrund einer konkreten Beschwerde – sei sie berechtigt oder unberechtigt – die Behörde tätig wird und dann „auch etwas findet".

Nicht außer Acht gelassen sollte im Übrigen allerdings auch der Aspekt werden, dass die Aufsichtsbehörden nach der gesetzlichen Bestimmung auch gehalten sind, die Verantwortlichen bei der Umsetzung der Datenschutzvorgaben zu beraten und zu informieren. Insoweit besteht auch eine Verpflichtung den Betroffenen mit Ratschlägen und Hinweisen zur Seite zu stehen.

11. Zusammenfassung

Die neuen Regelungen stellen eine Vielzahl von Anforderungen auf, die sicherlich in manchen Fällen nur schwer zu erfüllen sind. Als erste Schritte sind sicherlich erforderlich, dass sich die in jedem Betrieb verantwortlichen einen Überblick verschaffen, welche Anforderungen in ihrem Unternehmen zu erfüllen sind. Dies muss natürlich in jedem Unternehmen und in jedem Betrieb gesondert ermittelt werden. Es gibt hier auch keine „Musterlösungen".

Wichtig ist aber, dass zunächst einmal festgeschrieben wird, wer für welche Maßnahmen und welche Bereiche zuständig ist und auch die Verantwortung dafür trägt. Für alle Einzelpunkte die im Rahmen der DS-GVO zu erfüllen sind, muss ein federführend Verantwortlicher festgelegt werden. Aufgabe der Unternehmensleitung ist es, dies zu überwachen und zu kontrollieren und natürlich auch dafür Sorge zu tragen, dass geeignete Personen für die jeweiligen Tätigkeiten bestimmt werden.

Steinmarkt 12 • 93413 Cham
Telefon: 0 99 71/8 54 00 • **Telefax:** 0 99 71/4 01 80
E-Mail: info@kanzlei-am-steinmarkt.de • **www.kanzlei-am-steinmarkt.de**

Die gesetzliche Regelung sieht vor, dass Datenschutz „Chefsache" ist. Dies bedeutet, dass sich der Chef entweder selbst kümmern muss oder eine Person als Verantwortlichen benennen muss, der für seine Aufgabe auch geeignet ist. Die verschieden sich aus der Umsetzung der DS-GVO ergebenden Problemkreise können natürlich auch von verschiedenen Personen verantwortlich erledigt werden. Wichtig ist allerdings das klar ist, wer für was zuständig ist. Wichtig ist auch, dass sichergestellt wird, dass alle Mitarbeiter, die mit der Datenverarbeitung zu tun haben (dies sind in manchen Betrieben praktisch alle Mitarbeiter) über die von ihnen zu beachtenden Grundregeln verantwortlich informiert werden.

Betrieblich muss im Übrigen auch sichergestellt sein, dass die Anforderungen der DS-GVO auch ordnungsgemäß „fortgeschrieben" werden. Insbesondere im Hinblick auf sich ändernde technische Entwicklungen und sich ändernde Betriebsabläufe muss regelmäßig überprüft werden, ob die Dokumemtation des Datenschutzes noch den Realitäten und den gesetzlichen Anforderungen entspricht. Hier bedarf es der Vorgabe einer regelmäßigen Überprüfung der Maßnahmen.

Wer die notwendigen Maßnahmen ergreift, wird andererseits auch wenig Furcht vor Problemen oder Ansprüchen von Betroffenen haben müssen.