FAQs zur Umsetzung der EU-Datenschutz-Grundverordnung

Datenschutz ist momentan in aller Munde. Viele Unternehmen haben Sorge, die Anforderungen aus der EU-Datenschutz-Grundverordnung (DSGVO) und dem neunen Bundesdatenschutzgesetz (BDSG) nicht rechtzeitig bis zum 25. Mai 2018 umsetzen zu können. Vielerlei Hilfestellungen geben die Industrie- und Handelskammern durch Informationsveranstaltungen und individuelle Beratungen. Zudem gibt es Merkblätter/Newsletter, mit den einzelne Thermen aus der DSGVO erklärt und Hinweise für kleine Unternehmen bzw. Existenzgründer gegeben werden. Auch die Datenschutzaufsichtsbehörden in den Bundesländern geben Hilfestellung bei der Umsetzung. Sie finden Checklisten bzw. konkrete Branchenhinweise z. B. bei https://www.lda.bayern.de/de/index.html oder auch bei https://www.ldi.nrw.de/mainmenu_Service/submenu_Newsarchiv/Inhalt/Auf-dem-Weg-zur-Datenschutz-Grundverordnung/Auf-dem-Weg-zur-Datenschutz-Grundverordnung.html, wo ein Online-Test für Unternehmen vorhanden ist.
Die nachstehenden Fragen und Antworten („FAQs“) sind aus den zahlreichen Kontakten mit Unternehmen entstanden und sollen eine schnelle Hilfestellung bei konkreten Problemen geben.

Welche Arten von Daten sind durch die DSGVO geschützt?
Alle Arten von personenbezogenen Daten werden durch die DSGVO geschützt und dies unabhängig davon, um welche Kategorie von Personen es geht, also ob es sich hierbei um

- Mitarbeiter-,
- Geschäftspartner-, Kunden- oder
- Lieferantendaten handelt.

Für die DSGVO gilt wie für alle weiteren Datenschutzgesetze: Sie sind immer dann zu beachten, wenn Unternehmen mit sog. personenbezogenen Daten umgehen. Hierunter versteht man alle Informationen, die sich direkt oder indirekt (z. B. über eine Kennung) auf einen Menschen (sog. „identifizierte oder identifizierbare natürliche Person“ bzw. „betroffene Person“) beziehen lassen. Um Angaben über eine bestimmte Person handelt es sich, wenn die Daten mit dem Namen der betroffenen Person verbunden sind oder sich aus dem Inhalt bzw. dem Zusammenhang der Bezug unmittelbar herstellen lässt.
Beispielsweise:

- Name, Alter, Familienstand, Geburtsdatum
- Anschrift, Telefonnummer, E-Mail-Adresse
- Konto-, Kreditkartennummer
- Bonitätsdaten
- Kraftfahrzeugnummer, Kfz-Kennzeichen
- Personalausweisnummer, Sozialversicherungsnummer
- IP-Adresse
- genetische Daten und Krankendaten
- Werturteile wie zum Beispiel Zeugnisse
- Fotos

Sind Daten nicht personenbeziehbar (z. B. anonymisierte Statistikdaten), so sind Datenschutzgesetze nicht zu beachten.

Ich habe nur Firmenkunden. Muss ich den Datenschutz trotzdem beachten?
Datenschutz gilt grundsätzlich auch im Geschäftsverkehr mit anderen Unternehmen. Einzelangaben über juristische Personen, wie zum Kapitalgesellschaften oder eingetragene Vereine, sind keine personenbezogenen Daten. Etwas anderes gilt nur, wenn sich die Angaben auch auf die hinter der juristischen Person stehenden Personen beziehen, das heißt auf sie „durchschlagen“. Dies kann beispielsweise bei der GmbH einer Einzelperson oder bei einer Einzelfirma der Fall sein.

In der Regel haben Sie bei Firmenkunden einen Ansprechpartner und erheben z. B. Name, personalisierte E-Mail-Adresse, Funktion im Unternehmen usw. Hierbei handelt es sich wiederum um personenbezogene Daten, da eine natürliche Person identifizierbar ist.

Wird das Bundesdatenschutzgesetz (BDSG) neben der DSGVO weiterhin anwendbar sein?
Ja, die grundlegenden Vorschriften befinden sich in der DSGVO, aber z. B. zum betrieblichen Datenschutzbeauftragten oder zum Beschäftigtendatenschutz gibt das BDSG Konkretisierungen.
Das BDSG wird weiterhin gelten, allerdings deutlich reduziert. Die DSGVO gilt zwar unmittelbar für alle EU-Mitgliedstaaten und muss nicht erst in jeweils nationales Recht umgesetzt werden. Damit wollte der EU-Gesetzgeber eine Einheitlichkeit innerhalb der Mitgliedstaaten erreichten. Die DSGVO enthält aber mehr als 60 Öffnungsklauseln, die es den Mitgliedstaaten erlauben, wesentliche Aspekte national zu lösen, die nicht ausdrücklich allein der DSGVO vorbehalten sind. Daher gelten beide Regelwerke in einem komplizierten Regel-Ausnahme-System nebeneinander, was die Rechtsanwendung schwierig macht.

Gilt das Datenschutzrecht auch bei Dateien, die in Papierform verarbeitet werden?
Ja, die DSGVO unterscheidet nicht zwischen Papier- und elektronischer Verarbeitung. Bei einer papiergebundenen Datenverarbeitung muss aber eine strukturierte Sammlung von personenbezogenen Daten vorhanden sein. Kleine Notizen auf Blöcken oder „Post-it“ Aufkleber fallen also nicht darunter, wenn sie nicht geordnet abgelegt werden.

Werden auch Kleingewerbetreibende von der DSGVO erfasst?
Ja, alle Unternehmen müssen ihre Datenverarbeitungsvorgänge an die neuen Vorgaben der DSGVO anpassen. Dies gilt nicht nur für große, sondern auch für kleine Unternehmen. Kleine Unternehmen sind lediglich von einzelnen wenigen Pflichten ausgenommen; dies betrifft etwa unter Umständen die Pflicht zur Bestellung eines Datenschutzbeauftragten. Ansonsten müssen sämtliche Vorgaben umgesetzt werden, denn unter die DSGVO fällt jede Stelle (also auch jedes Unternehmen unabhängig von der Mitarbeiterzahl oder Branche), die personenbezogene Daten (z. B. Name, Vorname, Anschrift, Telefonnr., E-Mail-Adresse etc.) innerhalb der EU verarbeitet (z. B. erfassen, speichern, übermitteln, auslesen, verändern etc. von Daten).

Fallen auch außereuropäische Unternehmen unter die DSGVO?
Ja, wenn sie Waren oder Dienstleistungen anbieten oder die Verhaltensweisen ihrer Kunden in Europa zum Beispiel mittels „Profiling“ überwachen, wird die DSGVO angewendet.
Wann können Daten rechtmäßig verarbeitet werden?
Für die Rechtmäßigkeit gibt es mehrere Rechtsgrundlagen. Im geschäftlichen Verkehr mit Kunden kommen insbesondere vertragliche Vereinbarungen und die Einwilligung in Betracht. Daneben können auch Gesetze eine Verarbeitung rechtfertigen.

Brauche ich für jede Datenerhebung/-verarbeitung immer eine Einwilligung?
Nein, Sie benötigen für jede Verarbeitung von personenbezogenen Daten eine datenschutzrechtliche Rechtsgrundlage (etwa Vertrag oder Anbahnung eines Vertrags, Einwilligung, Interessenabwägung berechtigtes Interesse). Die Rechtsgrundlage kann in bestimmten Fällen auch eine Einwilligung sein (z. B. Anmeldung zum Bezug eines Newsletters, Geburtstagsliste von Mitarbeitern). Beruht die Datenverarbeitung auf einer vertraglichen Basis, um den Vertrag abzuwickeln, sind Einwilligungen für die Erhebung und Verarbeitung der Daten nicht erforderlich. Aber Vorsicht: Sollen die so erhobenen Daten für andere Zwecke als die Vertragsabwicklung verarbeitet werden (z. B. Verwertung der Daten für eine Studie oder Weitergabe der Daten an Dritte), so bedarf es einer Einwilligung für den neuen Zweck.

Wie sieht eine Einwilligung aus?
Eine wirksame Einwilligung muss

- über den Zweck der Verarbeitung informieren
- freiwillig erteilt sein, d. h. sie darf nicht an eine Bedingung gekoppelt sein
- eindeutig sein, also das Einverständnis muss deutlich werden und
- den Hinweis enthalten, dass sie mit Wirkung für die Zukunft jederzeit widerrufen werden kann.

Was bedeutet die Rechenschaftspflicht?
Sie bedeutet, dass Unternehmen in der Lage sein müssen, gegenüber Aufsichtsbehörden nachzuweisen, dass sie alle Vorgaben des Datenschutzes einhalten. Hierzu gehören auch die Datenschutzgrundsätze.

Darf ich die Daten meiner Mitarbeiter verarbeiten?
Die Daten von Stellenbewerbern, Mitarbeitern und ausgeschiedenen Mitarbeitern dürfen nach § 26 BDSG zur Begründung, Durchführung und Beendigung des Arbeitsverhältnisses verarbeitet werden. Geht eine Datenverarbeitung aber über diesen Zweck hinaus, z. B. die Veröffentlichung von Fotos auf der Firmenhomepage, ist darüber hinaus eine Einwilligung erforderlich. Eine Einwilligung muss immer freiwillig sein. Es dürfen bei Verweigerung also keine Nachteile drohen.

Was ist ein Datenschutzmanagement?
Zu einem Datenschutz-Managementsystem gehören u. a. die Führung eines Verzeichnisses von Verarbeitungstätigkeiten, ein Vertragsmanagement, Prozesse zur Meldung von Datenpannen und zur Wahrnehmung von Betroffenenrechten, ferner die Schulung von Mitarbeitern sowie deren Verpflichtung zur Verschwiegenheit und ein Datensicherheitskonzept.

Was ist ein Verzeichnis von Verarbeitungstätigkeiten?
Ein solches Verzeichnis ist eine Zusammenfassung von einzelnen Verarbeitungsvorgängen, bei denen personenbezogene Daten entweder automatisiert (=elektronisch) oder zunächst nicht automatisiert (=analog) verarbeitet werden, aber später in ein Dateisystem gespeichert werden sollen. Der Inhalt eines solchen Verzeichnisses ist gesetzlich geregelt. Das Verzeichnis muss wesentliche Angaben zur Verarbeitung beinhalten. Die Zwecke der Verarbeitung, die Beschreibung der betroffenen Datenkategorien und Personen sind aufzulisten. Eine bestimmte Form ist für das Verzeichnis nicht vorgesehen.

Wer muss ein Verzeichnis von Verarbeitungstätigkeiten anlegen?
Alle Unternehmen, die personenbezogene Daten automatisiert oder nicht automatisiert verarbeiten und sie in einem Dateisystem speichern oder speichern wollen, müssen ein Verzeichnis über die Verarbeitungen führen. Das Gesetz sieht eine Ausnahme vor: Unternehmen mit weniger als 250 Mitarbeitern sind von der Pflicht ein Verarbeitungsverzeichnis zu führen befreit. Aber auch nur dann, wenn die Verarbeitung selbst nicht ein Risiko birgt - das ist z. B. immer der Fall bei Scoring und Überwachungsmaßnahmen, die Verarbeitung nur gelegentlich erfolgt, und keine besonderen sensiblen Datenkategorien, wie z. B. Religions-, Gesundheitsdaten usw. betroffen sind. Die meisten Unternehmen verarbeiten regelmäßig Daten ihrer Mitarbeiter und Kunden, so dass die Ausnahmevorschrift in den meisten Fällen nicht greift und das Verarbeitungsverzeichnis geführt werden muss.

Muss ich auch noch Datensicherheit beachten?
Ja, die DSGVO verknüpft Datenschutz und Datensicherheit. Die personenbezogenen Daten, die in dem Unternehmen verarbeitet werden, müssen auch technisch geschützt werden, indem sog. technisch-organisatorische Maßnahmen getroffen sind. Sie hängen von der Schutzwürdigkeit der Daten und der Intensität der Verarbeitung ab. Aber schon aus eigenem Interesse sollte jedes Unternehmen seine Daten – ob personenbezogen oder nicht – ausreichend gegen Fremdzugriffe schützen. Das betrifft auch den Schutz vor Feuer und

Wasser, so dass – verschlüsselte - Sicherungskopien an einem anderen Ort aufbewahrt werden sollten.
Das Niveau der Datensicherheit ist abhängig vom Umfang der Datenverarbeitung, der Schutzwürdigkeit der Daten, ob sie online oder offline verarbeitet werden und den Zugriffsmöglichkeiten auf die Daten.

Was sind die wichtigsten Sofortmaßnahmen zur Umsetzung der DSGVO?
Zweck der DSGVO ist es vor allem, mehr Transparenz über Datenverarbeitungen gegenüber dem Betroffenen zu schaffen und dessen Rechte (Auskunft über gespeicherte Daten, Berichtigung oder Löschen von Daten) zu stärken. Gegenüber der Landesdatenschutzaufsicht muss das Unternehmen nachweisen, dass es aktiv Maßnahmen zur Einhaltung dieser Prinzipien und zur Sicherung der Datenverarbeitung umsetzt.

- Es muss ein Verarbeitungsverzeichnis mit folgenden Informationen erstellt werden: Den Zweck der Verarbeitung, die Kategorien der betroffenen Personen und die Kategorien der personenbezogenen Daten, die Kategorien von Empfängern, gegebenenfalls die Übermittlung von personenbezogenen Daten an ein Drittland, die vorgesehene Speicherdauer sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Datenverarbeitung. https://www.lda.bayern.de/de/kleine-unternehmen.html; https://datenschutz.sachsen-anhalt.de/informationen/internationales/datenschutz-grundverordnung/verzeichnis-der-verarbeitungstaetigkeiten-nach-artikel-30-ds-gvo/
- Die Datenschutzerklärung muss überarbeitet und um die Informationspflichten aus Artikel 13, 14 DSGVO ergänzt werden. Überwiegend handelt es sich um Informationen, die eine vollständige und ausführliche Datenschutzerklärung bisher auch enthalten hat. Neu ist anzugeben: die Rechtsgrundlagen der Datenverarbeitung und Hinweise zur vorgesehenen Speicherdauer.
- Werden die Daten durch einen Dienstleister im Auftrag des Unternehmens verarbeitet (Beispiele: Daten liegen in der Cloud, Newsletterversand über Agentur, Betreuung der Webseite), ist ein entsprechender Vertrag zur Auftragsverarbeitung mit dem Dienstleister zu schließen.
- Werden Daten aufgrund der Einwilligung des Betroffenen verarbeitet und entspricht diese Einwilligung den Anforderungen der DSGVO, das heißt, ist der oder sind die Zweck(e) zur Datenverarbeitung beschrieben und ist ein Hinweis auf die Freiwilligkeit und jederzeitige Widerrufbarkeit vorhanden? Andernfalls müssen die Einwilligungen neu eingeholt werden.
- Eine IT-Sicherheit ist aufzubauen (je nach Größe des Unternehmens im Umfang unterschiedlich)
- Schnelle Reaktionsmechanismen zur Meldung von Datenverstößen an die Aufsicht sind zu schaffen (künftig sind Datenschutzverletzungen binnen 72 Stunden zu melden)
- Ein Prozess zur Beantwortung von Betroffenenrechten ist einrichten (das sind die Rechte auf Auskunft, Berichtigung, Einschränkung oder Löschen von Daten)
- Betriebsvereinbarungen (sofern vorhanden) sind anzupassen.
- Risikobewertung der Verfahren
- Sensibilisierung der MitarbeiterInnen.

Gibt es besondere Stolperfallen für Startups?
Datenschutzfragen sollten bereits in der Gründungsphase geklärt werden. Wer Produkte wie Apps und Software entwickeln möchte, sollte den Grundsatz „Datenschutz durch Technik/Technikvoreinstellung“ beachten und datenschutzkonforme Produkte herstellen. Richtig umgesetzt, kann Datenschutz auch ein Marketingvorteil sein.

Wann müssen personenbezogene Daten gelöscht werden?
Personenbezogene Daten müssen grundsätzlich gelöscht werden, wenn diese für den Geschäftsprozess nicht mehr erforderlich sind, der Zweck, für den sie erhoben worden sind, also erfüllt ist. Die Löschung darf nicht vor Ablauf gesetzlicher Aufbewahrungsfristen

erfolgen, z. B. weil es Handelsbriefe (6 Jahre) sind oder steuerrechtliche Gründe (10 Jahre) eine Aufbewahrung vorschreiben. Grundsätzlich empfiehlt sich für jedes Unternehmen, ein sog. „Löschkonzept“ aufzusetzen. Dies ist zukünftig allein deswegen wichtig, um dem Grundsatz der Datenminimierung nach der DSGVO nachzukommen.

Benötigt mein Unternehmen einen Datenschutzbeauftragten?
Ja,

1. bei Unternehmen, deren Kerntätigkeit t in der systematischen Überwachung oder Verarbeitung besonderer personenbezogener Daten besteht
2. wenn der Verantwortliche/Auftragsverarbeiter in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (z. B. regelmäßige Kommunikation per E-Mail)

oder

3. wenn der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vornehmen, die einer Datenschutz-Folgeabschätzung nach Art. 35 DSGVO unterliegen. Das bedeutet, wenn besonders sensible Daten verarbeitet werden, wie zum Beispiel ethische Herkunft, politische Meinungen, Gewerkschaftszugehörigkeit, religiöse Überzeugungen, genetische Daten, biometrische Daten, Gesundheitsdaten, Daten zur sexuellen Orientierung usw. – dann hat das Unternehmen unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen einen Datenschutzbeauftragten zu benennen.

Das gilt nicht bei einem Versicherungsvermittler, der auch Gesundheitsdaten erhebt, da dies nicht seine Kerntätigkeit ist,

Was muss ich bei der Berechnung der Personenanzahl von 10 beachten?

- grundsätzlich sind sämtliche Personen, die mit der entsprechenden Verarbeitung beschäftigt sind, zu berücksichtigen, unabhängig von ihrem arbeitsrechtlichen Status als Arbeitnehmer, freie Mitarbeiter, Auszubildende, Praktikanten etc.
- eine zeitweise und kurzfristige Unter- bzw. Überschreitung der maßgeblichen Personenzahl ist unerheblich; wenn eine Person z. B. nur als Urlaubsvertretung mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt wird, ist diese nicht mitzuzählen, da sie diese Aufgabe nicht regelmäßig ausübt
- unerheblich ist, in welchem Umfang die beschäftigte Person diese Aufgabe wahrnimmt, also ob sie beispielweise als Teilzeitkraft diese Aufgabe ausübt (also in einem geringeren zeitlichen Umfang als eine Vollzeitkraft)

Automatisierte Verarbeitung meint IT-gestützte Datenverarbeitung, wie sie mittels Mainframe, Personal Computern (Desktop und Laptop Computern), aber mittlerweile auch mittels Smartphones, Tablet PCs und anderen mobilen Endgeräten erfolgt.
Der Begriff "ständig“ bedeutet nicht notwendig dauernd, verlangt aber, dass die Tätigkeit auf Dauer angelegt ist und die betreffende Person immer dann Daten verarbeitet, wenn es notwendig ist, selbst wenn die Tätigkeit nur in zeitlichen Abständen (z. B. monatlich) anfällt.

Wer kann betrieblicher Datenschutzbeauftragter werden?
Datenschutzbeauftragter darf nur sein, wer sowohl in rechtlicher als auch in technischer Hinsicht über die erforderlichen Kenntnisse verfügt und nicht Gefahr läuft, kraft seiner Position in dem Unternehmen einer Interessenkollision ausgesetzt zu sein. Damit kommen also weder Führungskräfte mit Personalverantwortung noch solche aus dem IT-Bereich (intern/extern) infrage. Der Datenschutzbeauftragte kann sowohl ein Mitarbeiter des Unternehmens als auch eine externe Person sein. Soweit ein Mitarbeiter zum Datenschutzbeauftragten ernannt wird, genießt dieser einen besonderen Kündigungsschutz und kann auch nur aus einem wichtigen Grund seines Amtes enthoben werden. Der besondere Kündigungsschutz reicht sogar bis zu einem Jahr nach Beendigung seiner Tätigkeit als Datenschutzbeauftragter fort. Ob eine Befristung der Ernennung rechtlich wirksam ist, ist sehr umstritten.

Was sind die Aufgaben eines Datenschutzbeauftragten?
Zusammengefasst lassen sich drei Bereiche von Pflichtaufgaben einteilen.

- Interne Aufgaben im Unternehmen (Unterrichtung und Beratung der Geschäftsführung und Mitarbeiter in datenschutzrelevanten Fragen; Überwachung der Einhaltung der rechtlichen Vorgaben; Sensibilisierung und Schulung von Mitarbeitern)
- Anlaufstelle im Verhältnis zur Aufsichtsbehörde und Zusammenarbeit mit dieser
- Anlaufstelle für betroffene Personen

Muss Datenschutz nur beachtet werden, wenn ein betrieblicher Datenschutzbeauftragter bestellt werden muss?
Nein, auch wenn ein betrieblicher Datenschutzbeauftragter nicht bestellt werden muss, ist der Datenschutz einzuhalten. Aufgaben, die klassischerweise dem Datenschutzbeauftragten obliegen, bspw. Unterstützung bei Erstellung des Verarbeitungsverzeichnisses, Schulung von Mitarbeitern, Beratung in datenschutzrelevanten Fragen, muss dann die Geschäftsführung selbst erledigen.

Kann die IHK einen Datenschutzbeauftragten/ externen Dienstleister empfehlen? Worauf ist bei der Beauftragung zu achten?
Es gibt Vereine und Berufsverbände, die konkrete Kontakte vermitteln können, wie etwa die Gesellschaft für Datenschutz und Datensicherheit e.V. (https://www.gdd.de/der-datenschutzbeauftragte) oder der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. (https://www.bvdnet.de/).
Bei der Auswahl eines externen Datenschutzbeauftragten empfiehlt es sich, mehrere Angebote mit Referenzen einzuholen und die Leistungen und Kosten zu vergleichen. Sie sollten für das Angebot vordefinieren, welche Leistungen Sie z. B. pauschal abgedeckt sehen wollen (z. B. Beratung im Standort-Alltag), oder die für die Erstellung/Überprüfung von Dokumenten (Verarbeitungsverzeichnis, Datenschutzerklärung, technisch-organisatorische Maßnahmen) bzw. Überwachung/Einhaltung datenschutzrechtlicher Vorschriften (z. B. Schulungen der Mitarbeiter, Auftragsverarbeitungen) usw. anfallen. Denkbar ist auch ein Kontingent an Beratungsstunden pro Jahr mit einem Pauschalbetrag abdecken zu lassen und Beratungsbedarf darüber hinaus mit einem vorher vereinbarten Stundensatz abrechnen zu lassen.
Rechtsanwälte aus dem Bereich Datenschutzrecht finden Sie bei der jeweiligen Rechtsanwaltskammer.

Wo kann ich mich zum Datenschutzbeauftragten schulen lassen?
Schulungen und Seminare zum Datenschutz können Sie im WIS - Weiterbildungs-Informations-System unter www.wis.ihk.de finden. Hier finden Sie neben Angeboten Ihrer IHK auch Angebote externer Anbieter, die Ihnen Informationen zum Datenschutz vermitteln können.

Was ist eine Datenschutz-Folgenabschätzung?
Eine Datenschutz-Folgenabschätzung ist eine Abschätzung der Folgen einer Datenverarbeitung mit voraussichtlich hohem Risiko für die Rechte und Freiheiten natürlicher Personen. Diese ist immer dann durchzuführen, wenn besonders sensible, personenbezogene Daten verarbeitet werden oder die Datenverarbeitung dazu bestimmt war, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, Leistungen oder seines Verhaltens zu bewerten. Sie hat den Zweck, rechtzeitig geeignete Maßnahmen ergreifen zu können, um das Risiko eines Schadens bei den Betroffenen zu minimieren.

Wie ist eine Datenschutz-Folgenabschätzung durchzuführen?
Die DSGVO bestimmt vier Mindestanforderungen bezüglich des Inhalts einer Datenschutz-Folgenabschätzung. Diese muss demnach enthalten:
- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen.
- Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck.

- Eine Bewertung der Risiken der Rechte und Freiheiten der betroffenen Personen.
- Die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen werden soll.

Bei der Durchführung einer Datenschutz-Folgenabschätzung ist zudem stets der Rat des Datenschutzbeauftragten einzuholen, sofern die gesetzliche Pflicht besteht, ihn zu ernennen.

Wie können die Informationspflichten bei telefonischer Datenerhebung oder Entgegennahme einer Visitenkarte sinnvoll umgesetzt werden?

Wird eine Visitenkarte übergeben, kann der Empfänger davon ausgehen, dass der Übergebende damit einverstanden ist, dass der Empfänger die Daten speichert. Aus dem Zusammenhang ergibt sich auch meist der Zweck der Übergabe - also Erhalt weiterer Informationen zu Produkten oder Dienstleistungen oder Einladung zu weiteren Veranstaltungen zu dem gleichen Thema. Wird mit dem Interessenten das erste Mal z. B. per Mail Kontakt aufgenommen, kann er über die Verarbeitung in Form der Informationspflicht aufgeklärt werden. Das kann auch mit einem Link in der Mail erfolgen, der auf die Informationspflicht auf der Internetseite verweist.

Kann ich die Daten meiner Kunden für Werbung verwenden?

Die Kunden, mit denen Sie bereits Kontakt haben (Bestandskunden) können Sie ohne deren Einwilligung Werbung zusenden. Die Kunden können allerdings dagegen Widerspruch einlegen.

Wollen Sie andere Personen bewerben, verlangt das Gesetz gegen unlauteren Wettbewerb (UWG), grundsätzlich eine postalische Ansprache. Werbung per Mail ist nur mit Einwilligung dieser Personen möglich.

Was bedeutet Auftragsverarbeitung (AV)?

Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung auch dann verantwortlich, wenn er dazu einen externen Dienstleister beauftragt. Das gilt insbesondere für die IT. Ob eine Webseite mit Kontaktformular oder die Betreuung der Kundendatenbank – andere Unternehmen sind dafür eingebunden. Sie haben Zugriff auf die personenbezogenen Daten, die der Auftraggeber für sein Unternehmen benötigt. In einem solchen Falle muss neben dem eigentlichen Auftrag, die konkrete Dienstleistung zu erbringen, noch eine Vereinbarung über die Auftragsverarbeitung geschlossen werden. Denn das erhöhte Gefahrenpotenzial für die Daten wegen des Zugriffs eines Dritten soll vertraglich geregelt werden. Aber Vorsicht! Von AV kann nur dann die Rede sein, wenn der Dienstleister streng nach einem zuvor definierten Verfahren vorgeht, keinen eigenen Gestaltungs- und Ermessenspielraum hat und gegenüber dem Auftraggeber im Hinblick auf die Ausführung der vereinbarten Tätigkeit weisungsgebunden ist. Kurzum: Wenn man den Dienstleister sinnbildlich als „verlängerte Werkbank“ des Auftraggebers betrachten kann. Darunter fallen auch z. B. sog. Trackingsysteme, mit denen nachvollzogen werden kann, wer welche Webseiten besucht hat. Gibt es zudem dadurch Auslandsbezug, weil das Tracking-Unternehmen seinen Sitz z. B. in den USA hat, müssen weitere datenschutzrechtliche Anforderungen erfüllt werden. Gleiches gilt für die Nutzung von Cloud-Anwendungen oder die Verwendung von social Plug-Ins auf den Webseiten, also die Einbindung sozialer Medien.

Liegt eine AV vor, so ist eine vorherige Einwilligung der Kunden, deren Daten verarbeitet werden, nicht erforderlich. Anders kann es hingegen sein, wenn keine AV vorliegt!

Keine Auftragsverarbeitung liegt vor, wenn die Daten an einen Dritten zur Durchführung einer Dienstleistung weitergegeben werden, z. B. an einen Steuerberater zur Abwicklung der gesamten Lohnbuchhaltung. Hier liegt es im berechtigten Interesse des Unternehmens, die dafür erforderlichen personenbezogenen Daten an den Dienstleister zu übermitteln.

Weitere Informationen finden Sie im Kurzpapier der Datenschutzkonferenz (DSK) https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/DSGVO_Kurzpapiere.html.

Muster dazu finden Sie hier: https://www.lda.bayern.de/media/muster_adv.pdf.

Was ist datenschutzrechtlich bei der Beauftragung eines Dienstleisters zu beachten?
Das beauftragte Unternehmen muss auch unter Datenschutzaspekten geeignet sein. Den Auftraggeber trifft hier eine Prüfpflicht. Nur solche Auftragsverarbeiter dürfen eingesetzt werden, die angemessene technische und organisatorische Maßnahmen zum Schutz der Daten getroffen haben und so eine Garantie für einen ausreichenden Datenschutz bieten. Als Beleg solcher Garantien können z. B. genehmigte Verhaltensregeln des Auftragsverarbeiters oder Zertifizierungen herangezogen werden.

Darf ich mein Geschäftslokal per Video überwachen?
Zur Wahrung des Hausrechts ist eine Videoüberwachung von Personen, die das Geschäftslokal betreten, zulässig, wenn sie insgesamt erforderlich ist, also kein weniger einschneidendes Mittel das Hausrecht wahren kann und die Überwachung nicht überraschend ist. Es muss jedoch frühzeitig, also z. B. am Eingang zum Geschäftslokal darauf hingewiesen und bekannt gegeben werden, wer die Videoüberwachung verantwortet. Wir auch das Gelände vor dem Geschäftslokal überwacht, gilt dasselbe: Hinweis auf die Überwachung und Angabe, wer überwacht.
Die Bilder aus der Videoüberwachung dürfen nur für kurze Zeit (ein – drei Tage) gespeichert werden, es sei denn, es können damit strafbaren Handlungen nachgewiesen werden. Dann dürfen aber nur die konkreten Sequenzen länger gespeichert werden, um sie den Strafverfolgungsbehörden zur Verfügung stellen zu können.
Eine reine Videoüberwachung ohne zusätzliche Auswertungsmöglichkeiten führt nicht dazu, dass ein betrieblicher Datenschutzbeauftragter bestellt werden muss.

Wer trägt die Verantwortung, wenn es zu datenschutzrechtlichen Verstößen kommt?
Die Verantwortung trägt das Unternehmen (sog. verantwortliche Stelle). Die DSGVO erweitert die Verantwortung des Unternehmens für Datenschutzverletzungen. Es haftet auch für Handlungen gesetzlicher Vertreter oder anderer Leitungspersonen des Unternehmens. sowie für Handlungen eines Beschäftigten oder eines eingeschalteten externen Beauftragten.
Ein Auftragsverarbeiter haftet selbst wie ein Verantwortlicher, wenn er gegen Weisungen des Auftraggebers verstößt und Daten des Auftraggebers für eigene Zwecke oder Zwecke Dritter verarbeitet. Neu werden zudem auch spezielle Haftungsregelungen für Auftragsverarbeiter im Falle von Datenschutzverletzungen eingeführt werden, d. h. Betroffene werden ihnen gegenüber bei Verstößen direkt Schadensersatzforderungen geltend machen können.

Darf ich die Daten meiner Mitarbeiter verarbeiten?
Nach DSGVO und BDSG unterliegen Beschäftigtendaten erhöhten Anforderungen. Dies wird u. a. durch umfassende Informations- und Dokumentationspflichten sichergestellt. Zum Beschäftigtendatenschutz gehören:

- die Einwilligung von Arbeitnehmern zur Verarbeitung persönlicher Daten, sofern die Datenverarbeitung nicht vom Arbeitsvertrag gedeckt ist
- die Übereinstimmung von Betriebs- oder Dienstvereinbarungen mit den Vorgaben der DSGVO und
- Regeln für den Datentransfer im Konzern (z. B. über die Rechtsgrundlage „berechtigtes Interesse“).

Müssen die Datenschutzerklärungen auf Website & Co. angepasst werden?
Unternehmen mit einer geschäftlichen Webseite müssen diese anpassen. Dazu gehören Hinweise zu:

- Rechtsgrundlage
- Zweck der Verarbeitung
- Dauer der Speicherung
- Betroffenenrechte
- Übermittlung an andere Stellen

Diese Angaben müssen zu allen Datenverarbeitungen, die auf der Homepage stattfinden, erfolgen, z. B.

- Logfiles,
  Cookies,
- Tracking- und Analysedienste (Google Analytics, Facebook-Pixel etc.),
  Registrierungsmöglichkeiten,
  Einbindung sozialer Netzwerke und
  Nutzung externer Zahlungsdienstleister (Klarna, PayPal etc.).

Auch ein eventuell vorhandenes Newslettersystem sollte im Zusammenhang mit dieser „Dateninventur“ unter die Lupe genommen werden. Möchte ein Kunde einen E-Mail-Newsletter online bestellen, so muss er in die Bestellung einwilligen. Die Einwilligung ist vom Unternehmen nachzuweisen, was beispielsweise über Double-Opt-In-Verfahren erfolgen muss.
Muster:
https://www.uni-muenster.de/Jura.itm/hoeren/lehre/materialien/musterdatenschutzerklaerung

Wie erfolgt eine Überprüfung durch die Datenschutzaufsicht?
Die Landesdatenschutzbeauftragten haben vielfältige Möglichkeiten, die Datenverarbeitung eines Unternehmens zu überprüfen. So kann die Aufsicht aus einem bestimmten Anlass – z. B. wegen einer Beschwerde eines Kunden, die Vorlage des Verarbeitungsverzeichnisses verlangen und dadurch die einzelnen Verfahren in dem Unternehmen überprüfen. Dazu kann die Aufsicht das Unternehmen aufsuchen oder sich die Unterlagen übersenden lassen. Nach der Prüfung erhält das Unternehmen Gelegenheit zur Stellungnahme, wenn es Beanstandungen gibt. Dier Aufsichtsbehörde prüft dann, welche Maßnahmen sie ergreift, die bis zur Verhängung von Bußgeldern oder zur Aufforderung, die Verarbeitung einzustellen, gehen können.

Wann muss ein Verstoß gemeldet werden?
Eine Verletzung des Schutzes personenbezogener Daten liegt vor, wenn z. B. der Verlust von Daten zu einem Risiko für die Rechte und Freiheiten der betroffenen Person führen kann. Der Verstoß muss innerhalb von 72 Stunden an die Datenschutzaufsicht gemeldet werden. Die Aufsichtsbehörden halten dafür ein Online-Meldeformular vor. Die betroffene Person muss ebenfalls informiert werden.

Mit welchen Sanktionen bei Verstößen ist zu rechnen?
Bei Verstößen gegen Datenschutzbestimmungen sieht die DSGVO empfindliche Geldstrafen vor. Die Höhe dieser Strafen kann bei besonders schlimmen Vergehen bis zu 20 Millionen Euro oder vier Prozent des letzten Jahresumsatzes betragen. Hier hat es im Vergleich zum bisherigen Recht erhebliche Verschärfungen gegeben.

Drohen mir Abmahnungen?
Inwieweit wettbewerbsrechtliche Abmahnungen von Mitbewerbern für Verstöße gegen den Datenschutz drohen, bleibt abzuwarten. Es empfiehlt sich aber, die eigene Datenschutzerklärung auf der Firmenhomepage an die DSGVO anzupassen. Denn diese ist nach außen transparent und somit der Einstieg für evtl. drohende Abmahnungen. Wenn Sie eine Abmahnung erhalten, unterzeichnen Sie zunächst keine Unterlassungserklärung. Wenden Sie sich an einen Anwalt oder an Ihre IHK für eine Beratung.