heyData

DATENSCHUTZ FÜR UNTERNEHMEN

ALLES WICHTIGE FÜR EINSTEIGER

INHALT

#01
Kurze Geschichte des Datenschutzes

#02
Datenschutz “in a nutshell”

#03
Der Datenschutzbeauftragte als Berater eines Unternehmens

#04
Welche Rechte haben natürliche Personen?

#05
Was passiert bei einer Datenpanne?

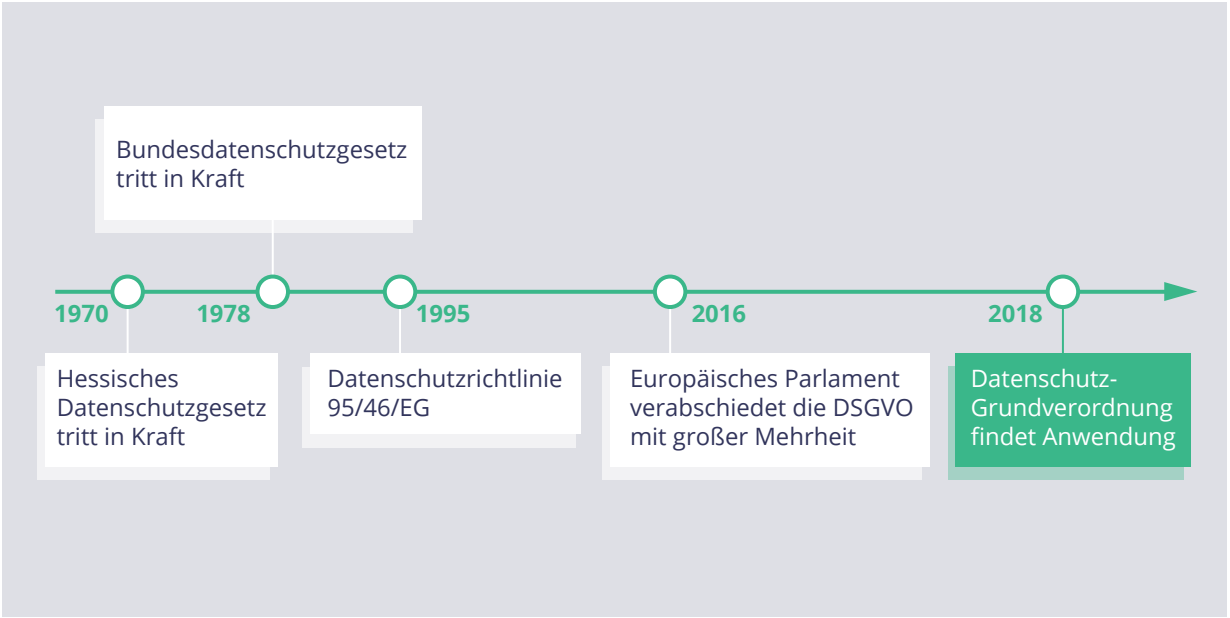
Auf den folgenden Seiten beantworten wir grundlegende Fragen rund um das Thema Datenschutz.

Falls Sie Nachfragen haben, kontaktieren Sie uns gerne unter **anfragen@heydata.eu** oder **+49 89 41325320**

#01

KURZE GESCHICHTE DES DATENSCHUTZES

Während früher Informationen ausschließlich manuell verarbeitet wurden und deshalb die Anzahl verarbeiteter Daten übersichtlich war, hat die mit der fortschreitenden technologische Entwicklung einhergehende Einführung einer Vielzahl an elektronischen Geräten das Sammeln immer mehr Daten ermöglicht. Schon früh hat die Öffentlichkeit in Deutschland nicht nur die wirtschaftliche Bedeutung dieser Datensammlungen erkannt, sondern auch, dass sie eine neue Dimension von **Eingriffen in die Privatsphäre von Personen** möglich machen. Parallel zur technischen Entwicklung und Digitalisierung stieg somit die Notwendigkeit, die Privatsphäre von natürlichen Personen zu schützen.
Um der Datenverarbeitung Grenzen zu setzen, traten 1970 als erstes Datenschutzgesetz der Welt das Hessisches Datenschutzgesetz und 1978 dann auf Bundesebene das **Bundesdatenschutzgesetz** in Kraft. Zudem ist seit einem Urteil des Bundesverfassungsgerichts 1983 die Existenz des „Rechts auf informationelle Selbstbestimmung“ anerkannt. Dieses räumt dem Einzelnen das Recht ein, über die Preisgabe und Verwendung seiner personenbezogenen Daten selbst zu bestimmen.
Während in Deutschland daher ein über Jahre gewachsenes System im Datenschutz Daten des Einzelnen schützte, waren entsprechende Regelungen in anderen Ländern der EU meist weniger ausgeprägt. Um ein gleiches Schutzsystem im gesamten Binnenmarkt zu erreichen, ist die **EU-Datenschutz-Grundverordnung (DSGVO)** als europäische Gesetzgebung 2016 geschaffen worden. Ab Mai 2018 finden die Bestimmungen in ganz Europa Anwendung - und Unternehmen sind unter Androhung von Bußgeldern verpflichtet, sie zu befolgen.



#02
DATENSCHUTZ “IN A NUTSHELL“

Datenschutz - Der Schutz personenbezogener Daten

Datenschutz stellt den Schutz natürlicher Personen in den Vordergrund. Ziel des Datenschutzes ist es, **Grundrechte und Freiheiten natürlichen Personen** zu schützen. Geschützt sind personenbezogene Daten. Personenbezogene Daten sind Informationen, welche sich direkt oder indirekt auf eine natürliche Person beziehen. Darunter fallen nicht nur Informationen wie Namen und E-Mail-Adressen, sondern auch technische Daten.

Der Anwendungsbereich ist deshalb weit. Unternehmen müssen deshalb wesentlich häufiger über Datenschutz nachdenken, als dies ein Laie erwarten würde. Jeder Umgang mit Daten - man spricht von Verarbeitung - setzt voraus, dass das Handeln auf eine rechtliche Grundlage gestützt werden kann. Sonst ist die Verarbeitung rechtswidrig.

Wer muss sich an Datenschutz halten?

An datenschutzrechtliche Vorgaben müssen sich nicht nur Unternehmen halten, sondern alle, die im nicht ausschließlich privaten Umfeld mit Daten umgehen, also auch z.B. **Stiftungen und Vereine**. Dabei gibt es keine Mindestgrenze an Mitarbeitern oder Mitgliedern, ab deren Erreichen Datenschutzregeln Anwendung finden: Datenschutzrechtliche Bestimmungen gelten sowohl für **Soloselbstständige** als auch für **internationale Konzerne**.

Es ist ratsam, sich möglichst **zeitnah nach Gründung** mit dem Thema Datenschutz auseinanderzusetzen, da Datenschutz-Verstöße sehr teuer werden können (siehe dazu „5. Was passiert bei einem Verstoß?"). Außerdem laufen Sie sonst Gefahr, Datenschutzprobleme zu übersehen, die bereits Ihr Geschäftsmodell betreffen.

Die Geschäftsführung ist verantwortlich

In Unternehmen ist die Geschäftsführung für die Einhaltung von Datenschutzbestimmungen verantwortlich - und kann von Behörden und Gerichten zur Rechenschaft gezogen werden. Die Einhaltung datenschutzrechtlicher Bestimmungen ist fortlaufend zu kontrollieren und zu dokumentieren. In der Praxis kommen der Geschäftsführung hier zahlreiche Dokumente zur Hilfe, die verpflichtend zu erstellen und zu aktualisieren vorzuhalten sind. Einen Teil dieser Dokumente wollen wir hier vorstellen.

Die Erstellung der Pflichtdokumentation nimmt viel Zeit in Anspruch, die Sie ebenso gut für die Betreuung Ihrer Kunden oder zur Kundenakquise aufwenden könnten. Wir von heyData nehmen Ihnen diese Arbeit fachmännisch ab.

Das Verzeichnis der Verarbeitungstätigkeiten gibt Übersicht

Jedes Unternehmen muss ein **Verzeichnis der Verarbeitungstätigkeiten (VVZ)** führen. In diesem dokumentiert das Unternehmen alle Tätigkeiten, bei denen Mitarbeiter im Unternehmen mit personenbezogenen Daten umgehen. Die Auflistung aller Tätigkeiten reicht aber nicht. Für jede Tätigkeit sind zusätzlich u.a. die verarbeiteten Kategorien von Daten (z.B. Name, E-Mail-Adresse, IP-Adresse), die Empfänger der Daten (z.B. interne Abteilungen oder externe Dienstleister) und die Aufbewahrungsfristen zu notieren. Ein richtig geführtes VVZ hat deshalb nicht drei, sondern 50 Seiten und mehr.

Übrigens ist das VVZ meist das erste Dokument, das sich Datenschutzbehörden bei Prüfungen vorlegen lassen. Hier sauber zu dokumentieren zahlt sich also aus. Natürlich reicht es nicht aus, das VVZ ein einziges Mal aufzusetzen. Vielmehr bedarf es der **regelmäßigen Aktualisierung**.

Viele Unternehmen denken, ein VVZ sei erst ab 250 Mitarbeitern Pflicht. Das ist falsch, weil das Datenschutzrecht eine Ausnahme vorsieht, die auf alle Unternehmen Anwendung findet: Die regelmäßig Datenverarbeitung. Denn darunter fällt schon das Schreiben von E-Mails.

Technische und Organisatorische Maßnahmen

Unter technischen und organisatorischen Maßnahmen werden alle **Schutzmaßnahmen** verstanden, mit denen Unternehmen personenbezogene Daten schützen.

In Betracht kommen viele Maßnahmen – von A wie einer Anweisung an Ihre Mitarbeiter, den Zugriff zu Ihrem Desktop-Computer zu sperren, wenn sie ihren Arbeitsplatz verlassen, bis Z wie einer zentralen Verwaltung von Benutzerrechten für Ihre Systeme.

Die von einem Unternehmen getroffenen Maßnahmen müssen im Verhältnis zu den betroffenen Daten stehen. Sie sind in einer Übersicht zu dokumentieren. Häufig ist diese Übersicht wichtig für Vertragspartner und **Voraussetzung für eine Zusammenarbeit**.

In unserem Audit prüft heyData Ihre Schutzmaßnahmen, schlägt weitere vor und gibt Tipps zur Datensicherheit. Das erforderliche Übersichtsdokument erstellen wir auch für Sie.

Termin vereinbaren

DIE WICHTIGSTEN BEGRIFFE IM ÜBERBLICK

PERSONENBEZOGENE DATEN
Daten, die Rückschlüsse auf eine natürliche Person erlauben. Sie sind deswegen unter besonderem Schutz, da jede Person ein Recht auf informationelle Selbstbestimmung hat.

PSEUDONYMISIERUNG
Identifizierende Merkmale werden durch einen Schlüssel ersetzt, so dass eine Zuordnung zu einer betroffenen Person nicht ohne diesen Schlüssel vorgenommen werden kann.

ANONYMISIERUNG
Einzelangaben können überhaupt nicht mehr einer bestimmten natürlichen Person zugeordnet werden.

BESONDERE PERSONENBEZOGENE DATEN
Daten aus denen rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Ansichten, Gewerkschaftszugehörigkeit oder sexuelle Orientierung hervorgehen sowie Gesundheits- genetische und biometrische Daten.

VERARBEITUNG
Jede Tätigkeit, die an personenbezogenen Daten durchgeführt wird; Erstellung, Sammlung, Speicherung, Transport, Verwendung, Änderung, Übertragung, Löschung usw., unabhängig davon, ob dies automatisiert erfolgt oder nicht.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN
Maßnahmen, die im Datenschutz die Sicherheit der Verarbeitung von personenbezogenen Daten gewährleisten sollen.

AUFTRAGSVERARBEITER
Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag einer anderen Stelle verarbeitet. Darunter fallen u.a. cloudbasierte Lohnbuchhaltung, CRMs, Hosting von Onlineshops und Webseiten uvm.

EINWILLIGUNG
Ein freiwilliges, für einen spezifischen Fall gegebenes, informiertes und eindeutiges Einverständnis zu einer Verarbeitung.

#03

DER DATENSCHUTZBEAUFTRAGTE ALS BERATER EINES UNTERNEHMENS

Der Datenschutzbeauftragte ist der ständige Berater eines Unternehmens in Datenschutzfragen. Er ist in der Datenschutzgrundverordnung fest vorgesehen. Dort steht auch, dass der Datenschutzbeauftragte unabhängig sein muss und die Einhaltung der Datenschutzgesetze überwacht.

Wer kann Datenschutzbeauftragter werden?

Das **Erfordernis der Unabhängigkeit** bringt es mit sich, dass Geschäftsführer, Vorstandsmitglied und die Leiter der Rechts- oder Personalabteilung nicht Datenschutzbeauftragte werden können. Häufig benennen Unternehmen einen Mitarbeiter zum Datenschutzbeauftragten, der nach seinem Arbeitsvertrag bereits andere Aufgaben erfüllen muss. Auch das ist problematisch. Denn der Datenschutzbeauftragte muss nicht nur genug Zeit zur sorgfältigen Erledigung seiner Aufgaben haben, sondern auch über das nötige Fachwissen verfügen. Das heißt nicht, dass ein Datenschutzbeauftragter Jura studiert haben muss. Er muss aber durch Weiterbildungen zu einem richtigen Kenner der Datenschutzgrundverordnung geworden sein und zusätzlich über technisches Verständnis verfügen.

Ohne tiefgehende Kenntnisse im Datenschutz kann ein Datenschutzbeauftragter auch nicht seinen Aufgaben, Mitarbeiter eines Unternehmens regelmäßig zu schulen und Fachfragen zu beantworten, nachkommen.

Vorsicht! Wenn ein Unternehmen einen Mitarbeiter zum Datenschutzbeauftragten macht, der nicht über das erforderliche Fachwissen verfügt oder der nicht unabhängig ist, riskiert es ein Bußgeld.

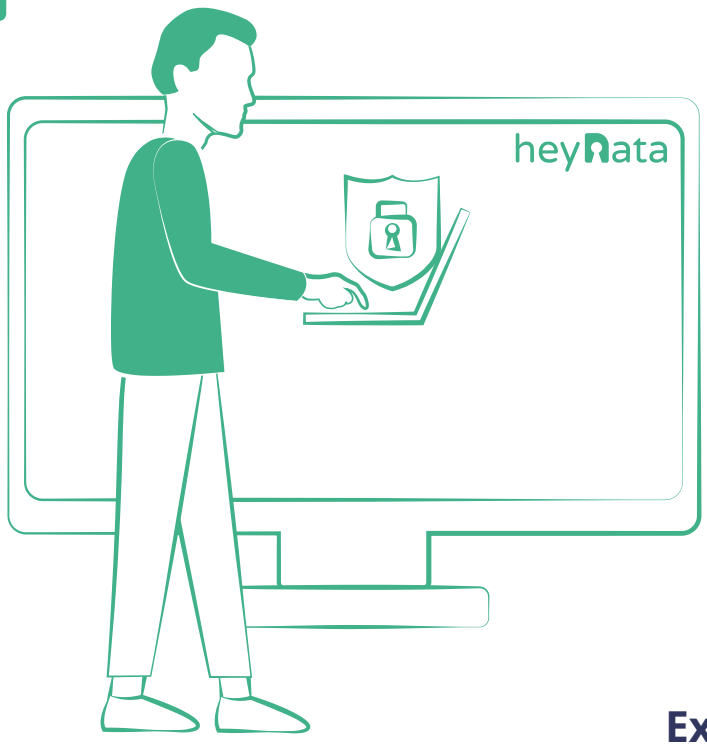
Brauche ich einen Datenschutzbeauftragten?

Die Frage ist ein wenig irreführend, weil Unternehmen häufig denken, dass sie ohne **Pflicht zur Beauftragung eines Datenschutzbeauftragten** auch nicht datenschutzrechtliche Vorgaben einhalten müssen. Das Gegenteil ist der Fall! Unternehmen ohne Datenschutzbeauftragten müssen selbst alle Pflichtdokumente im Datenschutz erstellen und aktualisieren, Mitarbeiter im Datenschutz schulen und Fachfragen lösen. Sonst drohen Bußgelder. Das Gesetz schreibt einen Datenschutzbeauftragten ab einer **Mitarbeiterzahl von 20** Mitarbeitern vor. Zu zählen ist nach „Köpfen" - eine Viertel-Stelle zählt deshalb als voller Mitarbeiter. Ebenso sind freie Mitarbeiter, die regelmäßig unterstützen, mitzurechnen. Es gibt zahlreiche weitere Unternehmen, die verpflichtet sind, einen Datenschutzbeauftragten zu benennen.

Die folgende Liste ist nur beispielhaft und mitnichten komplett:

- Unternehmen, die Videoüberwachung einsetzen
- Unternehmen, die neue Technologien (z.B. Künstliche Intelligenz oder Algorithmen) einsetzen
- Unternehmen, die in ihrer Haupttätigkeit besonders schutzwürdige Daten verarbeiten (z.B. Gesundheitsapps)
- Unternehmen, die in ihrer Haupttätigkeit natürliche Personen überwachen (z.B. über Standortdaten)

Ein Verstoß gegen die Pflicht einen Datenschutzbeauftragten zu benennen, wird von den Datenschutz-Behörden mit Bußgeldern sanktioniert. Das geringste uns bekannte Bußgeld belief sich in diesem Zusammenhang auf 5.000 EUR.



Externer oder interner DSB?

Interne Mitarbeiter dürfen nur zu Datenschutzbeauftragten werden, wenn sie über die nötige Erfahrung und das erforderliche Fachwissen verfügen. Dabei sollten Unternehmen nicht den Zeitaufwand unterschätzen, den das in Anspruch nehmen kann: Erst sind **Fachkenntnisse in mehreren Fortbildungen** zu erlangen, später regelmäßig aufzufrischen und auszubauen und natürlich kosten die Aufgaben eines Datenschutzbeauftragten auch Zeit.

Zudem fehlt es internen Datenschutzbeauftragten häufig an dem „Blick über den Tellerrand": Sie wissen zwar wie Datenschutzfragen im eigenen Unternehmen behandelt werden, aber nicht, welchen Weg andere Unternehmen wählen.

Schließlich sollten Unternehmen auch wissen, dass interne Datenschutzbeauftragte einen **Sonderkündigungsschutz** genießen – sie sind selbst aus betrieblichen Gründen so gut wie nicht kündbar.

Dagegen ist ein **externer Dienstleister als Datenschutzbeauftragter** ein Kenner der Materie. Da er mehrere Unternehmen als Datenschutzbeauftragter betreut, ist er sehr gut mit dem „business standard" vertraut und kennt die Antwort auf die meisten Fragen aus seiner täglichen Praxis. Und wenn etwas schief geht? Anders als ein interner Datenschutzbeauftragter, der nur privilegiert als Mitarbeiter (so gut wie gar nicht) haftet, verfügt ein externer Datenschutzbeauftragter über eine **Haftpflichtversicherung.**

#04

WELCHE RECHTE HABEN NATÜRLICHE PERSONEN?

Die Datenschutzgrundverordnung hat natürlichen Personen starke Werkzeuge an die Hand gegeben, mit denen sie den Umgang ihrer Daten durch Unternehmen enge Grenzen setzen können. Durch verstärkte Transparenz sollen natürliche Personen einen genauen Überblick über die Gesamtheit ihrer Daten erhalten und selbstbestimmt über die Nutzung der Daten entscheiden können. Natürliche Personen können gegenüber Unternehmen u.a. von folgenden Rechten Gebrauch machen:

Das Recht auf Auskunft

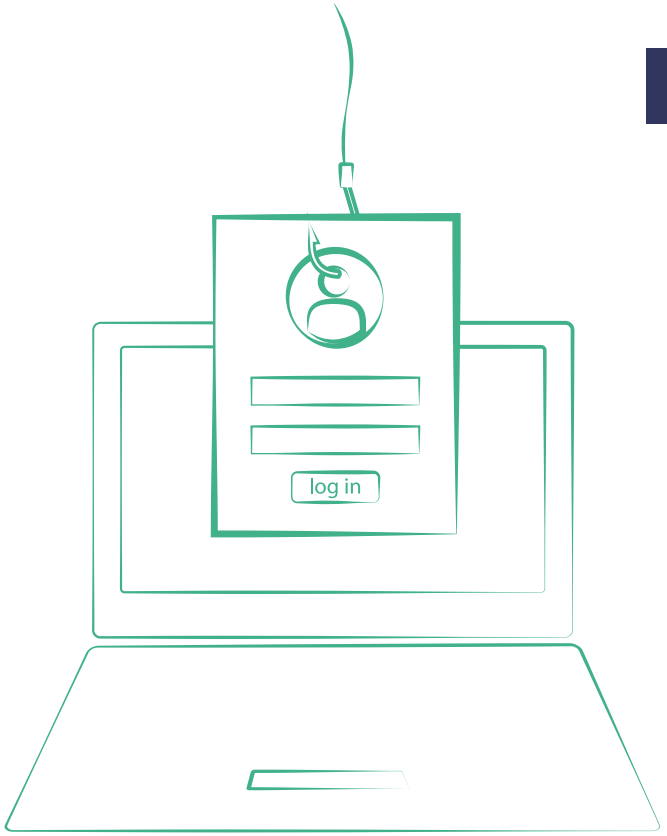
Natürliche Personen haben das Recht, von jedem Unternehmen zu erfahren, welche personenbezogenen Daten über ihre Person gespeichert sind oder auf andere Weise verarbeitet werden. Speichert ein Unternehmen keine Daten über eine Person, erhält die Person eine **Negativauskunft**. Neben der Auskunft, welche Daten verarbeitet werden, hat eine Person auch das Recht, weitere **Informationen zur Verarbeitung** zu erhalten, z.B. die Empfän-

Das Recht auf Löschung

In vielen Fällen können Betroffene von Unternehmen neben einer Auskunft auch verlangen, dass Unternehmen die über sie gespeicherten Daten löschen. Das ist z.B. der Fall, wenn Grundlage der Verarbeitung eine Einwilligung der Person ist. Die **Löschaufforderung** durch eine Person darf aber auch nicht dazu führen, dass Daten zu früh gelöscht werden. **Gesetzliche Aufbewahrungsfristen** (z.B. aus dem Steuerrecht) sind unbedingt zu beachten. Jede Löschanfrage bedarf deshalb einer sorgfältigen Bearbeitung. Außerdem darf ein Unternehmen Daten trotz Löschaufforderung länger speichern, wenn es auf sie angewiesen ist, z.B. um sich gegen mögliche Ansprüche des Anfragenden zu verteidigen.

Das Recht auf Datenübertragung

Schließlich kann eine Person auch verlangen, dass ihre Daten an andere Dienstleister oder Serviceanbieter weitergegeben werden. Dies hat in einem strukturierten Format zu erfolgen. Die **Anfrage auf Datenübertragung** trifft Unternehmen oft komplett ohne Vorplanung. Bereits wenn man technische Systeme aufsetzt, sollte man den Anspruch berücksichtigen.



#05

WAS PASSIERT BEI EINER DATENPANNE?

Jeder Verstoß gegen Bestimmungen des Datenschutzes ist eine Datenpanne. Die Spannweite möglicher Verletzungen ist weit: Sie reicht von einer einzigen E-Mail an einen falschen Empfänger bis zu einem Zugriff von Hackern auf tausende Kundendaten.

Das Vorgehen bei Verstößen

Eine Datenpanne ist deshalb schnell passiert. Wichtig ist, dass Mitarbeiter wissen, wie sie sich in diesem Fall verhalten. Vertuschen ist der falsche Weg und kann zu **hohen Bußgeldern** führen (mehr dazu unten).

Eine Datenpanne sollte direkt an den Datenschutzbeauftragten kommuniziert werden. Dieser schätzt das **Ausmaß der Panne** ein, empfiehlt Gegenmaßnahmen und berät die Geschäftsführung, ob die Datenpanne zu einer Meldepflicht führt. **Meldepflichten** können gegenüber Datenschutz-Behörden oder natürlichen Personen bestehen, deren Daten von der Panne betroffen sind.

Unternehmen haben zur Vornahme von Meldungen nur 72 Stunden Zeit. Hier ist schnelles Handeln und fachmännische Beratung gefragt. Ihr Datenschutzbeauftragter von heyData ist immer für Sie in Notfällen erreichbar.

Fordern Sie hier Ihren **Beratungstermin** an

oder kontaktieren Sie uns unter **anfragen@heydata.eu**

Welche Konsequenzen drohen bei einer Datenpanne?

Die 17 deutschen Datenschutz-Behörden überwachen die Einhaltung der Regelungen des Datenschutzes. Sie können Bußgelder verhängen. Nahezu täglich werden neue Bußgelder bekannt, die Behörden gegen Unternehmen verhängt haben.

Welche Höhe diese für Ihr Unternehmen erreichen können, haben wir in der folgenden Übersicht zusammengestellt:

z.B. keine datenschutzfreundliche Voreinstellung, keine angemessene Sicherheit, Datenpanne nicht gemeldet	z.B. Verstoß gegen Grundsätze der DSGVO, Vorschriften zur Einwilligung und Rechte der Betroffenen
2% *des weltweiten Jahresumsatzes* ODER 10 Mio. €*	4% *des weltweiten Jahresumsatzes* ODER 20 Mio. €*

**je nachdem was höher ist*

die genaue Höhe der Strafe hängt von diversen Faktoren ab, wie z.B. der Art des Schadens, der Schwere und Dauer der Datenschutzverletzung

2020 haben Datenschutz-Behörden in Deutschland Bußgelder in Höhe von 46 Mio. EUR verhängt. Die meisten Bußgelder ergingen nicht gegenüber großen Konzernen, sondern gegenüber Soloselbstständigen, kleinen Unternehmen und Vereinen.

Haben Sie Fragen zu diesem Thema oder allgemein zum Datenschutz?

Unsere Experten prüfen Ihr Unternehmen gern in einem unverbindlichen Beratungsgespräch auf Datenschutzlücken.

Im Vertrieb
Miloš Djurdjević
Geschäftsführer
milos@heydata.eu

Ihr Datenschutzberater
Rechtsanwalt Martin Bastius
Chief Legal Officer
support@heydata.eu