Zukunftsfähige, sichere Vernichtung von Daten und Dokumenten: Sind Sie bereit für die DSGVO?

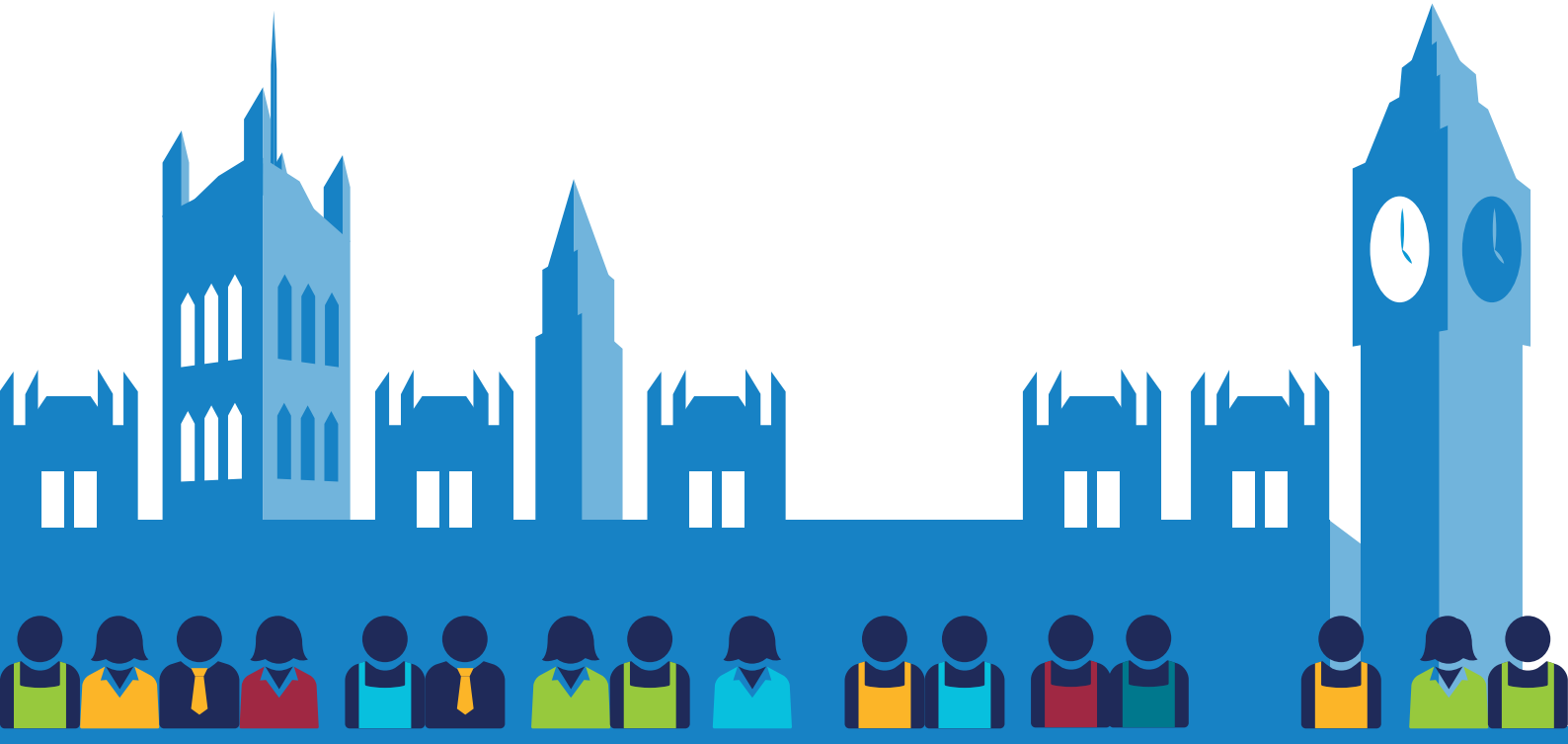
DSGVO-Regelung

Shred-it®

Inhalt

Einleitung

Die EU-Datenschutz-Grundverordnung (DSGVO) ist eine wichtige neue Regelung, die vom Europäischen Parlament und dem Rat der Europäischen Union verabschiedet wurde. Die Verordnung soll dafür sorgen, dass die Menschen in der Europäischen Union (EU) einen stärkeren und einheitlicheren Datenschutz erhalten. Das Europäische Parlament und der Rat der Europäischen Union wollen es den EU-Bürgern ermöglichen, zu kontrollieren, welche personenbezogenen Daten z.B. Unternehmen und öffentliche Stellen über sie besitzen. Auf diesem Weg ist die Verordnung ein wichtiger Schritt. Außerdem soll sichergestellt werden, dass für die Unternehmen selbst ein klarer, eindeutiger und einheitlicher Rechtsrahmen besteht, den sie beim Umgang mit personenbezogenen Daten befolgen können.



Die DSGVO ist in der EU ab dem 25. Mai 2018 anwendbar. Sie gilt nicht allein für Unternehmen, die in der EU ihren Sitz haben, sondern auch für solche Unternehmen, die mit personenbezogenen Daten von EU–Bürgern umgehen–ganz unabhängig davon, wo auf der Welt dieses Unternehmen seinen Sitz hat.

Auch wenn bis zur Anwendbarkeit der Verordnung noch Zeit bleibt, sollten Sie unbedingt sicherstellen, dass Ihr Unternehmen darauf vorbereitet ist. In diesem Informationsblatt erfahren Sie mehr darüber, was die DSGVO umfasst und wie sie sich auf Ihr Unternehmen auswirken wird. Wenn Sie bereits jetzt handeln, damit Ihr Unternehmen den kommenden Regelungen vollkommen entspricht, tragen Sie außerdem dazu bei, Ihr Unternehmen vor einer möglicherweise folgenschweren Verletzung des Datenschutzrechts zu schützen. So kann Ihre Organisation auch ihren Kunden, Partnern und Mitarbeitern versichern, dass Sie den Schutz deren Daten ernst nehmen – was die Glaubwürdigkeit Ihres Unternehmens stärkt.

Die EU-Datenschutz-Grundverordnung und was sie für Ihr Geschäft bedeutet

Was ist die DSGVO?

Die DSGVO ist eine weitreichende Regelung, die grundsätzlich für alle Unternehmen weltweit gilt, die personenbezogene Daten von Personen, die sich in der EU befinden, verarbeiten. Die Verordnung ist daher die erste, für die EU wirklich einheitlich eingesetzte Datenschutzregelung und führt das Konzept einer zentralen Anlaufstelle zum Thema Datenschutz ein: Jede Datenschutzbehörde in der EU kann nun gegen Organisationen in ihrem Zuständigkeitsbereich vorgehen. Sie führt eine neue und breitere Definition des Begriffs ‚personenbezogene Daten' ein, der nun z.B. auch Informationen zum Genmaterial und der geistigen Gesundheit einer Person umfasst.

Die Regelung führt zahlreiche neue Anforderungen an Unternehmen ein. Darunter fällt auch, dass Behörden, die personenbezogene Daten verarbeiten, einen Datenschutzbeauftragten (DSB) ernennen und Datenschutz-Folgenabschätzungen (DSFA) einführen müssen. Bevor Unternehmen nun ein Projekt starten, bei dem sie personenbezogene Daten verarbeiten, müssen sie eine Risikobewertung für den Datenschutz vornehmen. Unter gewissen Umständen sind DSFAs zwingend vorgeschrieben. Viele Privatunternehmen, die große Mengen an personenbezogener Daten verarbeiten, werden ebenfalls einen DSB ernennen oder beibehalten müssen.

Weitere Hauptgrundsätze und Merkmale der Regelung sind:

- Striktere Regeln für die Einwilligung in die Nutzung personenbezogener Daten: Da die Einwilligung zur rechtlichen Grundlage für die Datenverarbeitung gehört, müssen Unternehmen beweisen, dass ihnen eine Zustimmung jedes einzelnen vorliegt, um seine personenbezogenen Daten zu sammeln und zu speichern. Unternehmen werden auch nachweisen müssen, dass sie klar und eindeutig vor der Abgabe der Einwilligung informiert haben, wie sie die personenbezogenen Daten, die sie erhalten, verarbeiten und nutzen wollen.
- Das Recht auf Vergessenwerden wird eingeführt: Organisationen werden personenbezogene Daten nicht länger aufbewahren dürfen, als dies für den Verarbeitungszweck erforderlich ist. Sie müssen die ihnen vorliegenden personenbezogenen Daten grundsätzlich auch dann unverzüglich löschen, wenn sie von der Person dazu aufgefordert werden, auf die sich die Daten beziehen.
- Anforderungen an Informationstechnologiesysteme: Die Regelung sieht vor, dass die von den Organisationen eingesetzte Software gezielt Funktionen zum Schutz der personenbezogenen Daten vorsieht. Von Beginn an muss jede Software dem Ansatz des, Datenschutzes durch Technik' *(privacy by design)* entsprechend auf den Schutz der Daten der betroffenen Person ausgerichtet sein.
- Auftragsverarbeiter, die für Verantwortliche personenbezogene Daten verarbeiten, müssen ebenfalls neue Regelungen beachten: Sie treffen nach der DSGVO neue Pflichten wie z.B. das Führen des Verzeichnisses von Verarbeitungstätigkeiten.

Was sind personenbezogene Daten?

Die DSGVO bezieht sich auf personenbezogenen Daten und sie beschreibt sehr detailliert, was diese umfassen: Dies reicht von schriftliche Daten bis hin zu genetischem Material. Die Erwägungsgründe heben auch hervor, welche Auswirkungen die technologischen Veränderungen auf die Datensammlung haben. Man sollte beachten, dass Online-Kennungen wie die IP-Adresse als personenbezogene Daten betrachtet werden können.

Den meisten Unternehmen und Organisationen liegen personenbezogene Daten vor, die unter dieser Gesetzgebung geschützt werden müssen. Einige Beispiele, die auf die meisten Unternehmen und Organisationen zutreffen, sind Gehaltsabrechnungen, Kundenkontaktinformationen, Personaldaten und E-Mails.

Was ist der Unterschied zwischen einem „Verantwortlichen“ und einem „Auftragsverarbeiter“?

Ein „Verantwortlicher“ ist eine Organisation oder Person, die entweder allein oder gemeinsam mit anderen Personen darüber entscheidet, wie und zu welchem Zweck Daten verarbeitet werden sollen. Ein „Auftragsverarbeiter“ ist jemand, der kein Mitarbeiter des Verantwortlichen ist und im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet. Falls Ihr Unternehmen zum Beispiel online Produkte verkauft, dann können Sie eine Dritte mit der Betreuung des Online-Shops oder der Bearbeitung von Kundenzahlungen betrauen. Ihr Unternehmen ist dann der Verantwortliche und der Dritte ist der Auftragsverarbeiter.

Aus der DSGVO ergeben sich für Auftragsverarbeiter neue rechtliche Pflichten, da sie nun auch selbst für die Nichteinhaltung der Regelung oder einen Gesetzesverstoß belangt werden können. Nach noch aktuell gültigem Recht trifft die Verantwortung hierfür bislang nur den Verantwortlichen.

Weshalb ist die DSGVO wichtig?

Die DSGVO ist wichtig, weil sie den Schutz jedes Einzelnen stärkt, wenn es darum geht, wie die personenbezogenen Daten gesammelt, gespeichert, verarbeitet und genutzt werden. Sie ist jedoch auch für Unternehmen von Bedeutung: Wird gegen die DSGVO verstoßen, kann dies empfindliche Bußgelder für die Verantwortlichen zur Folge haben.

Datenschutzbehörden werden berechtigt, Bußgelder zu verhängen, die – abhängig vom Datenschutzverstoß - bis zu **20 Mio. €** oder **4 Prozent des weltweiten Umsatzes** (je nachdem, welcher Betrag höher ist) betragen können.

Organisationen sollten jedoch nicht allein die rechtlichen und finanziellen Konsequenzen in Betracht ziehen – ein Verstoß gegen die DSGVO kann sich auch extrem rufschädigend auswirken. Eine Verletzung des Datenschutzes oder ein Verstoß gegen die Regelung kann dazu führen, dass Kunden ihr Vertrauen in Sie verlieren, und erhebliche negative Folgen für Ihr Geschäft haben.

Wer muss sich daran halten?

- Alle Organisationen, die in der EU tätig sind – einschließlich Organisationen, die in der EU Niederlassungen/Büros betreiben, aber außerhalb der EU registriert sind
- Jede Organisation, die Personen, die sich in der EU befinden, ihre Dienste anbietet (und zwar Unabhängig davon, wo die Organisation ihren Sitz hat.

Wie unterscheidet sie sich von der bisherigen Gesetzgebung?

Zurzeit folgt der Datenschutz in der EU der Datenschutzrichtlinie, die seit 1995 in Kraft ist. Diese reguliert die Verarbeitung personenbezogener Daten in der EU. EU-Richtlinien müssen jedoch (anders als EU-Verordnungen) in den einzelnen Mitgliedstaaten durch nationale Gesetze umgesetzt werden. Im Vereinigten Königreich gilt derzeit zum Beispiel das britische Datenschutzgesetz von 1998, in Deutschland hingegen das Bundesdatenschutzgesetz (BDSG). Die Umsetzung der EU-Datenschutzrichtlinie erfolgte jedoch nicht in allen EU-Mitgliedstaaten einheitlich. Das hat dazu geführt, dass es in Sachen Datenschutz zwischen den EU-Mitgliedstaaten erhebliche Unterschiede bei der Regelung und Durchsetzung im Bereich des Datenschutzrechtes gibt.

Die EU-Datenschutzrichtlinie wird durch die DSGVO abgelöst, wenn sie im Mai 2018 anwendbar wird. Auch die jeweiligen Gesetze in den EU-Mitgliedsstaaten, wie das britische Datenschutzgesetz von 1998 oder das BDSG werden durch die überlagert: Sie sind nicht mehr anwendbar, soweit sie mit der DSGVO in Widerspruch stehen. In allen Mitgliedsstaaten der EU gilt dann unmittelbar die DSGVO.

Wer wird die DSGVO durchsetzen?

Die DSGVO wird von Aufsichtsbehörden (AB) durchgesetzt. Jeder Mitgliedsstaat muss eine AB als Regulierungsstelle einrichten, die z.B. Beschwerden anhört, Anfragen nachgeht und Bußgelder verhängt. Die ABs der einzelnen EU.-Mitgliedstaaten müssen zusammenarbeiten. Falls sich beispielsweise herausstellt, dass ein Unternehmen mit britischem Hauptsitz in einer seiner deutschen Niederlassungen rechtswidrig mit Daten verarbeitet, dann wäre die AB in Deutschland vorrangig zuständig. Allerdings könnte sie mit der britischen AB gemeinsame Untersuchungen zu dem beanstandeten Vorgang anstellen.

Was passiert bei einer Verletzung des Schutzes personenbezogener Daten?

DSGVO sind Organisationen verpflichtet, den zuständigen ABs bestimmte Arten der Verletzung des Schutzes personenbezogener Daten zu melden. Dazu gehören Verletzungen, aus denen sich wahrscheinlich eine Gefährdung der Rechte von Personen ergibt. Dies ist der Fall, wenn eine Verletzung für jemanden z. B. zu finanziellen Verlusten, einer Rufschädigung oder einem Vertrauensbruch führt. Die Organisation muss der zuständigen Aufsichtsbehörde die Verletzung binnen 72 Stunden nach Bemerken der Verletzung melden; ansonsten kann gegen sie ein Bußgeld von bis zu 10 Mio. € oder zwei Prozent ihres weltweiten Umsatzes verhängt werden.

In einigen Fällen müssen Unternehmen die Verletzungen gegen den Datenschutz auch den Personen melden, deren personenbezogene Daten davon betroffen sind. Dies gilt für Fälle, bei denen die Verletzung voraussichtlich zu einem hohen Risiko für die Rechte der jeweiligen Person führt.

Welche Rechte räumt die DSGVO jedem Betroffenen ein?

Das Recht auf Information

Betont die Notwendigkeit von Transparenz bei der Datenverarbeitung.

Das Recht auf Auskunft

Jeder kann sich informieren lassen, welche seiner personenbezogenen Daten verarbeitet werden.

Das Recht auf Richtigstellung

Das Recht, personenbezogene Daten korrigieren zu lassen, falls sie falsch oder unvollständig sind.

Das Recht auf Löschung

Auch bekannt als das Recht auf Vergessenwerden, d. h. jeder kann fordern, dass seine persönlichen Daten gelöscht oder entfernt werden.

Rechte in Bezug auf automatisch getroffene Entscheidungen und Profiling

Schützen vor Entscheidungen, die ohne menschliches Eingreifen getroffen wurden und nachteilig sein könnten.

Das Recht auf Datenübertragbarkeit

Jeder kann von ihm zur Verfügung gestellte personenbezogene Daten herausverlangen.

Das Recht auf Widerspruch

Jeder kann der Verarbeitung seiner personenbezogenen Daten widersprechen.

Das Recht auf Einschränkung der Verarbeitung

Das heißt, Unternehmen können die personenbezogenen Daten speichern, aber nicht weiter verarbeiten, wenn der Betroffene die Einschränkung verlangt.

Fragen Sie den Fachmann:

Helena Brown

Experte für die Rechtsprechung in Sachen Datenschutz

Helena Brown ist Leiterin des Datenteams in der globalen Anwaltskanzlei Addleshaw Goddard. Als anerkannte Datenschutzexpertin verfügt sie über weitreichende Erfahrung bei der Gewährleistung des Datenschutzes im gewerblichen Umfeld, einschließlich der Unterstützung bei Datenanliegen wie DSGVO-Konformitäts-Audits, Marketing- und Einverständnisprüfungen, internationalen Datentransfers, Datenbeschwerden und -untersuchungen. Helena verfügt darüber hinaus über Erfahrung bei der Technologiebeschaffung, komplexen Wirtschaftsverträgen und dem Schutz und der Verwertung von geistigem Eigentum einschließlich Datenbankrechten im Zusammenhang mit Datenschutz.

Was sind die Hauptunterschiede zwischen der DSGVO und den aktuellen Datenschutzgesetzen?

Änderung	Beschreibung der Änderung	Praktische Auswirkung
Einwilligung	Die Einwilligung ist ein wichtiger Bestandteil der DSGVO, denn sie stärkt die Rechte jedes Einzelnen, über die Art der Verarbeitung seiner Daten zu bestimmen. Wenn die Datenverarbeitung auf einer Einwilligung beruht, muss der Verantwortliche beweisen können, dass diese eindeutig und freiwillig erfolgte. In die Nutzung zu Werbezwecken muss explizit eingewilligt werden (‚Opt-in'-Methode).	Einwilligungsprozesse und -texte aller Plattformen und Medien müssen überprüft werden. Einwilligungen, die nur durch Deaktivierung vorausgefüllter Auswahlkästchen abgelehnt werden können (‚Opt-out-Methode'), sind nach dem 25. Mai 2018 nicht mehr wirksam erteilt.
Verletzungen des Datenschutzes	Datenverantwortliche müssen bestimmte Verletzungen des Schutzes personenbezogener Daten der zuständigen Behörde ohne unnötige Verzögerung, möglichst binnen 72 Stunden nach Bemerken, melden. Falls jemandem durch die Verletzung ein Schaden entstanden ist, kann diese Person vom Verantwortlichen oder vom Auftragsverarbeiter Schadenersatz verlangen.	Verfahren des Vorfallmanagements für Datenschutzverletzungen müssen geprüft und falls erforderlich erweitert werden. Die Mitarbeiter müssen darin geschult werden, eine Verletzung des Datenschutzes zu erkennen und sie den Vorgesetzten zu melden. Verträge müssen geprüft und falls erforderlich geändert werden, um die Anforderungen an die Meldung und den Schadenersatz bei Datenschutzverletzungen zu erfüllen.
Datenüber-tragbarkeit	Die DSGVO führt das neue Recht auf Datenübertragbarkeit ein. Aufgrund dieses Rechts muss der Verantwortliche nach Aufforderung die personenbezogenen Daten, die ihm von einer Person übermittelt wurden, in einem strukturierten, gängigen und maschinenlesbaren Format an die Person zurückgeben, damit sie einem anderen Datenverantwortlichen übermitteln kann.	Es wird wichtig werden, genau zu verstehen, wo und in welchem Format Daten gespeichert werden, um die Weitergabe und den Erhalt von Daten von einer Drittpartei zu vereinfachen. Hiervon sind nur personenbezogene Daten betroffen, die die betroffene Person dem Datenverantwortlichen zu Beginn der gegenseitigen Beziehung bereitgestellt hat.

Änderung	Beschreibung der Änderung	Praktische Auswirkung
Datenschutz-beauftragter	Es kann erforderlich werden, einen Datenschutzbeauftragten (DSB) einzusetzen. Der DSB sollte der höchsten Managementebene unterstehen und muss über alle Datenschutzfragen und -probleme in der Organisation unterrichtet werden.	Wer sollte Datenschutzbeauftragter werden? Kann er auf Vorstandsebene berichten?
Neue oder erweiterte Rechte – Auskunfttsanfragen durch betroffene Personen	Die Frist, in der solchen Anfragen nachgekommen werden muss, wurde von 40 Kalendertagen auf einen Kalendermonat gekürzt. Es dürfen keine Gebühren hierfür erhoben werden. Neu sind auch de Rechte auf Datenübertragbarkeit, auf Vergessenwerden und auf Datenlöschung.	Das Verfahren für Auskunftsanfragen muss geprüft und aktualisiert werden. Zusätzliche Ressourcen können erforderlich sein. 25 % der betroffenen Personen werden nämlich erfahrungsgemäß durch Gebühren davon abgehalten, eine Auskunftsanfrage zu stellen.
Datenschutz durch Technik (privacy by design)	Bei der Entwicklung, Gestaltung oder Nutzung von Produkten, Diensten oder Anwendungen, die die Verarbeitung personenbezogener Daten umfassen, müssen Verantwortliche und Auftragsverarbeiter den Schutz personenbezogener Daten durch Technik sicherzustellen.	Change-Management-Verfahren müssen geprüft werden, um bei der Entwicklung oder Änderung von Produkten, Diensten, Systemen und Prozessen die Einhaltung des Datenschutzes durch Technik sichergestellt werden kann.
Datenschutz-Folgenabschätzungen (DSFA)	Die DSVGO macht es verpflichtend, in bestimmten Situationen DSFAs durchzuführen. DSFAs müssen eine Beschreibung der Verarbeitung sowie des Verarbeitungszwecks beinhalten und müssen alle Risiken für die personenbezogenen Daten sowie die Rechte und Freiheiten betroffener Personen bezeichnen. Außerdem müssen Maßnahmen und Sicherungen zur Milderung dieser Risiken benannt werden.	DSFAs müssen dort eingeführt werden, wo neue Technologien für Hochrisiko-Datenverarbeitung oder die weitreichende Verarbeitung sensibler Daten zum Einsatz kommen. Dies gilt auch, wenn automatische Verarbeitungsverfahren systematisch und umfassend zur Verhaltensbeurteilung, -analyse oder -prognose genutzt werden.
Datenschutzer-klärungen	Laut der DSGVO müssen Datenschutzerklärungen transparent, klare und einfach formuliert werden und einfach zugänglich sein.	Online-Datenschutzerklärungen und Produkt-AGBs müssen geprüft und aktualisiert werden, um sie klarer, transparenter und einfacher zugänglich zu machen.
Profiling	Niemand darf Gegenstand einer Entscheidung sein, die ausschließlich anhand automatischer Prozesse getroffen wurde, z. B. Profiling.	Aktivitäten, die auf Profiling beruhen oder Profiling nutzen, müssen ermittelt werden und es ist festzustellen, ob sie einer Einwilligung bedürfen.
Verzeichnis von Verarbeitungstätigkeiten	Verantwortliche und Auftragsverarbeiter müssen grundsätzlich ein Verzeichnis der Verarbeitungsaktivitäten führen.	Das Verzeichnis muss entsprechend erstellt werden.
Das Recht auf Löschung	Jeder hat das Recht, zu verlangen, dass seine personenbezogenen Daten gelöscht werden. Der Verantwortliche muss personenbezogene Daten auf Anfrage löschen, sofern nicht ausnahmsweise ein Rechtsgrund für die Aufbewahrung der Daten besteht.	Es müssen Prozesse zur Datenlöschung eingeführt werden, damit Daten nicht unbegrenzt lange gespeichert werden. Datenbestände müssen auf ihre Löschreife hin durchgesehen werden.
Das Recht auf Widerspruch	Jeder muss auf sein Recht hingewiesen werden, z.B. Direktwerbung zu widersprechen. Auf dieses Recht muss ausdrücklich, klar formuliert und getrennt von anderen Informationen hingewiesen werden.	Abmeldemethoden müssen überprüft werden.

Was bedeuten der Grundsatz der Rechenschaftspflicht und das Transparenzgebot?

Aufgrund des in Art. 5 Abs. 2 DSGVO neu formulierten Grundsatzes zur Rechenschaftspflicht müssen Sie auf transparente Weise nachweisen können, dass Sie die Datenschutzgrundsätze der DSGVO einhalten.

Organisationen sollten:

- angemessene technische und organisatorische Maßnahmen ergreifen, um die Einhaltung der DSGVO sicherzustellen und nachzuweisen. Darunter gehören z.B. interne Datenschutzrichtlinien, Mitarbeiterschulungen und interne Audits.
- relevante Dokumentationen zu Verarbeitungsaktivitäten pflegen.
- einen Datenschutzbeauftragten benennen (falls gesetzlich erforderlich).
- Maßnahmen einleiten, die den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) entsprechen. Die Maßnahmen können z.B. Folgendes umfassen:
  - *Datenminimierung;*
  - *Pseudonymisierung;*
  - *Transparenz;*
  - *Erlaubnis der Überwachung der Verarbeitung durch betroffene Personen; und*
  - *Fortlaufende Schaffung und Verbesserung von Schutzfunktionen.*
- Datenschutz-Folgenabschätzungen durchführen (falls gesetzlich erforderlich).

Welche rechtlichen Folgen hätte eine Nichtbeachtung der DSGVO?

Die Behörden können für bestimmte Verstöße gegen die DSGVO Bußgelder in Höhe von 20 Mio. € oder 4 % des weltweiten Jahresumsatzes verhängen, je nachdem, welcher Betrag höher ist.

Für andere Verstöße hingegen liegt der maximale Bußgeldrahmen bei bis zu **10 Mio. €** oder **2 % des weltweiten Jahresumsatzes**, je nachdem, welcher Betrag höher ist.

Neben den Bußgeldern, die für Verletzungen des Datenschutzes verhängt werden können, enthält die DSGVO auch das Recht von betroffenen Personen, für Schäden, die ihnen aus solchen Fällen entstehen, Schadenersatz zu verlangen. **Ein Verantwortlicher oder Auftragsverarbeiter könnte also bei einer Datenschutzverletzung sowohl zur Zahlung von Schadensersatz als auch von Geldbuße verpflichtet sein.**

Die DSGVO ermöglicht es betroffenen Personen, von Verantwortlichen und Auftragsverarbeitern Ersatz für alle Schäden zu fordern, die ihnen aufgrund einer Verletzung des Datenschutzes entstanden sind.

Verantwortliche, gegen die Schadensersatzansprüche erhoben werden, können bei einer Auftragsverarbeitung vom Auftragsverarbeiter die gesamte oder einen Teil der zu zahlenden Summe zurückverlangen, falls tatsächlich der Auftragsverarbeiter ganz oder teilweise für die Verletzung verantwortlich ist. Dies gilt aber entsprechend auch für den Auftragsverarbeiter, sollte er von dem Betroffenen in Anspruch genommen werden.

Aufgrund der rechtlichen Änderungen liegt es im Interesse sowohl von Verantwortlichen als auch Auftragsverarbeitern, detaillierte Vereinbarungen über die Auftragsverarbeitung abzuschließen, um im Konfliktfall gerüstet zu sein.

Wie kann die sichere Vernichtung personenbezogener Daten Organisationen helfen, die DSGVO einzuhalten?

Organisationen sollten über eine Richtlinie zur Datenverarbeitung verfügen, da die DSGVO vorsieht, dass betroffene Personen über Einzelheiten der Datenverarbeitung Auskunft verlangen können. Aufgrund des zuvor angesprochenen Grundsatzes der Rechenschaftspflicht müssen Organisationen belegen können, dass sie ihre eigenen Richtlinien zur Datenverarbeitung befolgen. Diese müssen auch die sichere Vernichtung personenbezogener Daten vorsehen, um eine Einhaltung der DSGVO zu gewährleisten.

Weshalb ist es wichtig, dass Organisationen weltweit jetzt bereits handeln?

Die DSGVO hat eine extraterritoriale Wirkung, d. h. dass das Gesetz für alle Organisationen gilt, die personenbezogene Daten Personen, die sich in der EU befinden, verarbeiten - ganz egal, wo in der Welt die Organisation ihren Sitz hat. Die DSGVO ist ab dem 25. Mai 2018 anwendbar, daher sollten Unternehmen dringend die internen Prüfungen vornehmen, um eine Einhaltung der DSGCO sicherzustellen.

Ich würde Unternehmen das folgende Vorgehen empfehlen:

- Verwendung neuer Einwilligungstexte, die den Anforderungen der DSGVO entsprechen;
- Feststellen, ob Datenschutz-Folgenabschätzungen erforderlich sind;
- Datenaudits durchführen und Gutachten erstellen (lassen);
- Überprüfung der Richtlinien zur Datenverarbeitung und Datenspeicherung;
- Überprüfung interner Systeme und Kontrollmechanismen, einschließlich Zugangskontrollen;
- Mapping von Datenflüssen und internationalen Transfers;
- Neuformulierung von Richtlinien und Standards für Datenschutz und Sicherheit;
- Überprüfung von:
  - *Materialien, die sich mit der Mitarbeiterüberwachung befassen (z. B. Richtlinien/Verhaltensregeln bezüglich Sicherheitskameras);*
  - *Verträge mit IT-Anbietern über die Beachtung von Regeln bezüglich internationaler Transfers von personenbezogenen Daten;*
  - *Prozessen für Auskunftsanfrage durch betroffene Personen gemäß der DSGVO;*
  - *Mitarbeiterverträgen, Mitarbeiterrichtlinien, Verhaltensregeln, anderen relevanten HR-Materialien, einschließlich Agenturverträge und Bewerberrichtlinien;*
  - *Vereinbarungen über Auftragsverarbeitungen;*
  - *der Art der verarbeiteten Daten, um festzustellen, ob diese als personenbezogene Daten im Sinne der DSGVO gelten;*
  - *Website-AGBs.*

Aktiv werden

Organisationen müssen die DSGVO befolgen, sobald diese am 25.05.2018 anwendbar ist. Daher sollten Sie sich unbedingt im Voraus darauf vorbereiten, die Anforderungen der DSGVO zu erfüllen. Jetzt haben Sie noch Zeit, sich mit Anwälten sowie Fachleuten auf dem Gebiet des Datenschutzes und der Informationssicherheit zu beraten, um sicherzugehen, dass bereits alle Ihre Fragen beantwortet und gelöst sind, wenn es soweit ist.

Darüber hinaus ist ein geschützter Arbeitsplatz aber auch entscheidend, um mögliche rechtliche und finanzielle Risiken sowie Gefährdungen des Unternehmensrufes abzuwenden. Organisationen sollten sicherstellen, dass alle Informationen über Kunden, Mitarbeiter und Partner sicher bearbeitet, gespeichert und entsorgt werden.

Ihr Weg zur Einhaltung der DSGVO: Bewährte Praktiken zum Schutz des Arbeitsplatzes

Die erforderlichen Maßnahmen zur Implementierung der DSGVO können viel Zeit beanspruchen, da sich Ihre Mitarbeiter an neue Verantwortungen gewöhnen müssen. Es ist daher von großer Wichtigkeit, dass Sie so früh wie möglich anfangen, bewährte Praktiken einzuführen, so dass bei Ihnen bereits alles reibungslos läuft, wenn die DSGVO anwendbar ist. Folgende Maßnahmen können Sie ergreifen.

Verfassen Sie eine robuste Informationssicherheitsrichtlinie und aktualisieren Sie diese regelmäßig.

Laut der DSGVO können Datenschutzbehörden jederzeit verlangen, Ihre Datenschutzrichtlinien und-verfahren zu prüfen.

In der Informationssicherheitsrichtlinie sollten enthalten sein:

- Datenkategorien und wie lange sie vor der sicheren Vernichtung gespeichert werden sollten
- Methoden zur Vernichtung von Informationen
  - *Denken Sie sowohl an physisch vorhandene Daten (z. B. Drucksachen) und an elektronische Daten (z. B. Daten in einer Cloud) sowie an die Geräte zur Speicherung elektronischer Daten (z. B. Laptops, USBs – sowohl verwendet als auch redundant)*
  - *Denken Sie an das Recht auf Vergessenwerden und wie Sie sicher alle personenbezogenen Daten vernichten können, die Sie zu einer Person gespeichert haben, falls Sie dazu aufgefordert werden. Neben der Vernichtung von Papierunterlagen müssen Sie ggf. auch ein Verfahren zur Vernichtung von Daten auf Festplatten vorweisen*
- Wie Sie exakt aufzeichnen, welche Daten vernichtet worden sind.

Bestimmen Sie eine Person oder ein Team zur Aufsicht über den Datenschutz

Organisationen, die eine umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen durchführen oder in großem Umfang sensible personenbezogene Daten oder Daten bezüglich strafrechtlicher Verurteilungen und Straftaten verarbeiten, müssen einen Datenschutzbeauftragten ernennen. Es hat sich jedoch bewährt, auch dann eine Person in Ihrer Organisation zum Verantwortlichen für Informationssicherheit zu bestimmen, wenn dies nicht gesetzlich vorgeschrieben ist. In größeren Organisationen ist es wichtig, eine interne Revision zu etablieren, die den Erfolg Ihrer Maßnahmen prüft.

Führen Sie Datenschutz-Folgenabschätzungen (DSFA) ein

Falls Sie nicht bereits DSFAs durchführen, führen Sie sie jetzt in Ihre Organisation ein. Dabei handelt es sich im Wesentlichen um Risikobeurteilungen, bei denen Bereiche ermittelt werden, in denen personenbezogene Daten bei der Verarbeitung gefährdet sein könnten. Führen Sie DSFAs in der Frühphase von Projekten durch, damit Sie den Datenschutz von Beginn an im Blick haben.

Entwickeln Sie ein Meldeverfahren bei Datenschutz-verletzungen

Gewisse Verletzungen des Datenschutzes müssen binnen 72 Stunden gemeldet werden, was keine lange Zeit ist, wenn man gerade dabei ist, ein Problem zu lösen. Mit der Einrichtung eines bekannten und allgemein nachvollziehbaren Meldeverfahrens und eines Reaktionsplans sind Sie besser in der Lage, rasch zu handeln, wenn es zu einer Datenschutzverletzung kommt. Dies hilft Ihnen, sich der DSGVO entsprechend zu verhalten, aber es hilft Ihnen auch, das Problem rasch zu beheben und den Schaden zu begrenzen.

Unterstützen Sie die Mitarbeiter mit hilfreichen Richtlinien beim Schutz vertraulicher Daten

ühren Sie eine Clean-Desk-Richtlinie ein (d. h. alle Informationen werden weggeschlossen, wenn Mitarbeiter nicht am Platz sind). So sinkt die Wahrscheinlichkeit, dass vertrauliches Material verloren geht. Mit einer Shred-it®-All-Richtlinie (bei der alle auf Papier gedruckten Informationen vor der Entsorgung vernichtet werden) müssen die Mitarbeiter nicht selbst entscheiden, welche Informationen vertraulich sind und welche nicht. Statt Ihre Mitarbeiter Material mit einem Büroschredder vernichten zu lassen, entscheiden Sie sich lieber für einen Anbieter von sicherer Datenvernichtung wie Shred-it®. Wir vernichten Dokumente mit Kreuzschnitt, damit weder unberechtigte Personen noch Organisationen sie wieder zusammensetzen können. Herkömmliche Büroschredder schneiden Dokumente oft nur in Streifen, was weniger sicher ist. Außerdem könnten Dokumente vor dem Vernichten ungesichert herumliegen, da diese Aufgabe für Mitarbeiter oft nicht die höchste Priorität hat.

Schulen Sie das Personal regelmäßig zu Richtlinien und wichtigen Themen in Sachen Datenschutz

Jeder in einer Organisation spielt eine wichtige Rolle, wenn es um die Einhaltung der DSGVO geht. Alle Mitarbeiter sollten die DSGVO kennen und wissen, was sie bedeutet, damit sie sich ihrer Zuständigkeiten beim Schutz der Daten anderer Personen bewusst sind und wissen, welche Maßnahmen sie dafür ergreifen müssen. Diese Entwicklung muss von der Unternehmensspitze ausgehen. Geschäftsleitung und Vorgesetzte müssen Datenschutz aktiv zur Priorität machen und in der Organisation eine Kultur der Sicherheit erzeugen.

Suchen Sie rechtliche Beratung

Gehen Sie bei etwas so Wichtigem wie der DSGVO kein Risiko ein. Suchen Sie Rat bei einem juristischen Expertenteam, das auf den Bereich Datenschutz spezialisiert ist, damit Sie absolut sicher sein können, dass Sie alle Auswirkungen auf Ihr Unternehmen verstehen. Denken Sie daran, dass die DSGVO weitreichende Folgen hat – und zwar nicht nur für Organisationen in der EU, sondern auf der ganzen Welt.

Wie Shred-it® helfen kann

Der geschützte Arbeitsplatz von Shred-it®

Unser integriertes Produkt- und Service-Angebot – einschließlich Akten- und Datenträgervernichtung, Sicherheitsrichtlinien für den Arbeitsplatz als Stationen einer sicheren Überwachungskette – ist dafür gemacht, an jedem einzelnen Tag die Dinge zu schützen, die wirklich zählen.

Sichere Vernichtung von Dokumenten und Festplatten:

- Verfahren für eine sichere, lückenlose Überwachungskette
- Erstellung eines Vernichtungszertifikats nach jeder Dienstleistung
- Lösungen, die auf den Bedarf Ihrer Organisation zugeschnitten sind

Beratung und Fachwissen

- Geschulte Fachleute für Datenschutz
- Führen Sie in Ihrer Organisation eine Datenschutzumfrage durch, um Risiken für die Informationssicherheit aufzudecken.
- Hilfreiche Ressourcen finden Sie auf shredit.de/mediencenter

Wir schützen das, was wirklich zählt.

shredit.de
0800 0281160

Shred-it®