Einführung in die neue

DATENSCHUTZ-GRUNDVERORDNUNG

DSGVO

Was bedeutet die neue Datenschutz-Grundverordnung für Sie und Ihr Unternehmen?

Cordery® Legal.Compliance

Fellowes® WORK BETTER™

Worum geht es überhaupt und wie ist der derzeitige Stand?

Die Europäische Union (EU) hat ihre Datenschutzverordnung geändert. Die Änderungen sind nun rechtsverbindlich und treten am 25. Mai 2018 in der EU in Kraft. Die neue Datenschutz-Grundverordnung (DSGVO) gilt pauschal, von öffentlichen Behörden bis hin zu kleinen und mittleren Unternehmen. Die Veränderungen haben Einfluss darauf, wie wir alle in Zukunft unsere Geschäfte tätigen. Dieses Dokument gibt Ihnen eine grundlegende Einführung in die DSGVO und geht speziell darauf ein, wie sie sich auf die Arbeit im Büro auswirkt.

Worum geht es beim EU-Datenschutz?

In der EU gibt es bereits Verordnungen zur Erfassung und Verarbeitung personenbezogener Daten. Jeder, der personenbezogene Daten erfasst oder verarbeitet, muss diese vor missbräuchlicher Verwendung schützen und eine Reihe rechtlicher Anforderungen erfüllen. Die DSGVO ist eine Erweiterung der bestehenden Verordnung.

Gilt die neue Verordnung für elektronische Daten und für Hartkopien?

Ja. Die DSGVO gilt für elektronische Daten (wie E-Mails und Datenbanken) und für Hartkopien (mit wenigen Ausnahmen). Das bedeutet, dass wir auch in Bezug auf Papierakten dafür verantwortlich sind, diese sicher aufzubewahren und zu entsorgen (beispielsweise mithilfe eines dafür geeigneten Aktenvernichters), wenn wir sie nicht mehr benötigen.

Mit welchen Bußgeldern muss mein Unternehmen bei einem Verstoß gegen die Verordnung rechnen?

Im Rahmen der neuen Datenschutzverordnung können die Aufsichtsbehörden hohe Bußgelder verhängen – bis zu einem Höchstbetrag von 20 Millionen Euro bzw. 4 % des weltweiten Jahresumsatzes eines Unternehmens, je nachdem, welcher Betrag höher ist. Auch wenn nicht jeder Verstoß direkt mit dem Höchstsatz geahndet wird, ist das Risiko, eventuell ein Bußgeld zu kassieren, überhaupt keine Option – wir müssen alle sicherstellen, uns an die Verordnung zu halten.

Müssen Unternehmen mehr tun als bisher?

Ja. Im Rahmen der neuen Verordnung hat jedes Unternehmen mehr Verantwortung und Pflichten. Unternehmen müssen vor allem technische und organisatorische Maßnahmen vorsehen, um sicherzustellen, dass Daten ordnungsgemäß verarbeitet werden. Um das korrekte Sicherheitsniveau zu bestimmen, müssen Sie die Risiken berücksichtigen, die mit der Verarbeitung verbunden sind, speziell bei einer versehentlichen oder ungesetzlichen Vernichtung. Auf Anfrage müssen Sie den Aufsichtsbehörden auch nachweisen können, welche Maßnahmen Sie zum Schutz der Daten ergriffen haben. Ein wichtiger Teil besteht darin zu kontrollieren, an wen die personenbezogenen Daten gesendet werden. Dazu müssen Sie auch die Prozesse von Dritten überprüfen, mit denen Sie zusammenarbeiten, beispielsweise Versandunternehmen, Aktenvernichtungsunternehmen und Zeitarbeitsfirmen.

Gibt es Beispiele für Unternehmen, die hier Fehler gemacht haben?

- **Sich nicht an die Datenschutzverordnung zu halten, kann teuer werden.** Vor kurzem hat die britische Datenschutzaufsichtsbehörde ICO ein Bußgeld von 100.000 Pfund gegen eine Kommunalbehörde verhängt, die keine Sicherheitsmaßnahmen gegen den versehentlichen Verlust oder die versehentliche Vernichtung von Daten nachweisen konnte. Im betreffenden Fall fand der neue Eigentümer eines leer stehenden Gebäudes, das früher von der Kommunalbehörde genutzt worden war, Dokumente mit personenbezogenen Daten von rund 100 Personen (darunter schutzbedürftige Erwachsene und Kinder). Zu diesem Fehler kam es, als die Kommunalbehörde in ein anderes Gebäude umzog und beim Auszug versehentlich Unterlagen zurückließ.

- In den Niederlanden verhängte die Datenschutzaufsichtsbehörde Bußgelder gegen einige Betreiber öffentlicher Verkehrsmittel, weil bestimmte Transaktionsdaten dort länger als erforderlich aufbewahrt wurden. Die Betreiber waren von der Aufsichtsbehörde zuvor dazu angehalten worden, die Transaktionsdaten entweder zu löschen oder zu anonymisieren, und hatten beschlossen, die Daten weiter aufzubewahren und zu anonymisieren. Die Anonymisierungstechniken waren jedoch in mindestens einem Fall unzureichend, sodass ein Betreiber ein **Bußgeld in Höhe von 125.000 Euro zahlen musste**.

- Aus Spanien sind mehrere Fälle bekannt, in denen die Datenschutzaufsichtsbehörde Bußgelder verhängte. In einem Fall wurden Unterlagen mit personenbezogenen Daten in Mülleimern oder auf der Straße entsorgt. In mindestens einem Fall waren die Unterlagen nur teilweise mithilfe von Aktenvernichtern vernichtet worden, in anderen Fällen waren die Unterlagen überhaupt nicht ober nur unzureichend vernichtet worden.

Muss ich bei allem, was ich tue, an den Datenschutz denken?

Ja. Der Datenschutz muss bei allen Ihren Prozessen berücksichtigt werden. Unternehmen müssen beispielsweise Maßnahmen vorsehen, die standardmäßig sicherstellen, dass nur relevante personenbezogene Daten zweckentsprechend und nicht über den Zweck hinausgehend verarbeitet werden. Sie müssen sich also immer folgende Fragen stellen:

- Benötige ich diese personenbezogenen Daten?
- Muss ich sie zu diesem Zweck verarbeiten?
- Muss jeder, der darauf zugreifen kann, auch Zugriff darauf haben? (Das könnte zum Beispiel bedeuten, dass Unterlagen, die nur die Personalabteilung sehen darf, unter Umständen in einem Aktenschrank aufbewahrt werden müssen, zu dem nur Mitarbeiter der Personalabteilung einen Schlüssel haben.)
- Sind die Daten eventuell nicht mehr aktuell?

Ist für die Verarbeitung von Daten die Einwilligung der Betroffenen erforderlich?

Ja. Ganz allgemein muss für die Verarbeitung personenbezogener Daten ein legitimer Grund vorliegen. Falls die Verarbeitung der Daten von einer Einwilligung der betroffenen Person abhängt, muss diese Einwilligung im Rahmen der neuen Verordnung freiwillig, konkret, informiert und unzweideutig erteilt werden. Stillschweigen, Abwahl oder Inaktivität gelten nicht als Einwilligung. Stattdessen ist ein aktiver Prozess wie beispielsweise das Setzen eines Häkchens in ein Kästchen erforderlich. Unternehmen müssen außerdem nachweisen können, dass tatsächlich eine Einwilligung erteilt wurde. Stellen Sie sicher, dass in Ihrem Unternehmen Prozesse in Kraft sind, die alle diese Anforderungen erfüllen.

Gibt es neue Rechte?

Ja. Es wurde eine Reihe neuer Rechte eingeführt, unter anderem folgende:

- Das Recht auf Vergessenwerden – damit haben Betroffene das Recht, die Löschung ihrer personenbezogenen Daten zu verlangen
- Das Recht auf Datenübertragbarkeit – damit haben Betroffene das Recht, die Übertragung ihrer personenbezogenen Daten in einem gängigen Format zu verlangen
- Widerspruchsrecht – das beinhaltet das Recht der Betroffen, einem Profiling zu widersprechen. Auch wenn personenbezogene Daten für die Direktvermarktung genutzt werden, ist ein Widerspruch möglich

Diese neuen Rechte zu implementieren, stellt Unternehmen vor Herausforderungen, auch wenn darauf hingewiesen werden sollte, dass es gewisse Ausnahmen gibt; hier sollten sich Unternehmen unbedingt rechtlich beraten lassen.

Was ist mit Personen, die ihre Daten einsehen möchten?

Das Auskunftsrecht, das den Betroffenen das Recht einräumt, ihre Daten einzusehen, bleibt im Rahmen der neuen Verordnung bestehen. Damit kann eine Person verlangen, auf die über sie gespeicherten Daten zuzugreifen. Im Rahmen der neuen Verordnung müssen Auskunftsanfragen innerhalb eines Monats nach Erhalt der Anfrage beantwortet werden (auch wenn die Frist unter Umständen um zwei Monate verlängert werden kann). Unternehmen dürfen auch keine Gebühr mehr für die Beantwortung von Auskunftsanfragen erheben. Die Zahl der Auskunftsanfragen ist in den letzten Jahren erheblich gestiegen. Wenn sie in Zukunft dann gebührenfrei sind, ist mit einer weiter steigenden Zahl zu rechnen. Angesichts der Zunahme speziell von E-Mail- und Cloud-Anwendungen ist die Bearbeitung von Auskunftsanfragen mittlerweile kostenintensiv und komplex.

Ein wichtiger Teil der zukünftigen Datenschutzstrategie eines Unternehmens muss daher in der Einrichtung angemessener Prozesse für die Bearbeitung von Auskunftsanfragen bestehen.

Muss ich einen Datenschutzbeauftragten ernennen?

Möglicherweise. Im Rahmen der DSGVO müssen öffentliche Behörden einen Datenschutzbeauftragten ernennen. Dies trifft unter bestimmten Umständen auch für Unternehmen zu. Auch hier empfiehlt es sich, rechtlichen Rat einzuholen, je nachdem, was Sie tun und wo. In Anbetracht der Bedeutung, die der Einhaltung von Datenschutzgesetzen heute zukommt, kann es selbst für mittelständische Unternehmen, die regelmäßig Daten verarbeiten, empfehlenswert sein, einen Datenschutzbeauftragten zu ernennen, auch wenn dies rechtlich nicht unbedingt erforderlich sein sollte.

Muss ich Datenschutzverletzungen melden?

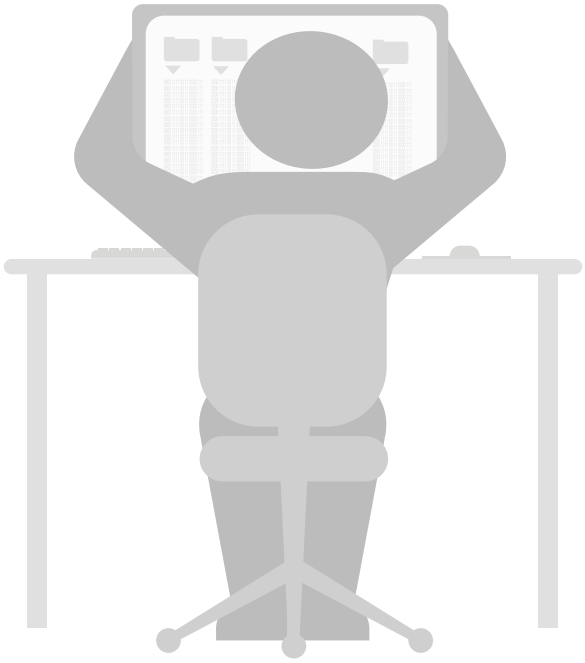
Ja. Zu gewährleisten, dass Daten sicher sind, ist einer der Grundpfeiler der neuen Verordnung; dazu zählt auch der Umgang mit Datenschutzverletzungen.

Datenschutzverletzungen betreffen viele Situationen, unter anderem Vernichtung, Verlust, Änderung, unbefugte Preisgabe oder unbefugten Zugriff auf personenbezogene Daten.

Datenschutzverletzungen müssen der zuständigen Datenschutzaufsichtsbehörde unverzüglich und (sofern machbar) spätestens 72 Stunden nach Bekanntwerden der Verletzung gemeldet werden (einschließlich der zur Minderung getroffenen Maßnahmen). Auch die von der Datenschutzverletzung betroffenen Personen sind umgehend zu benachrichtigen (auch wenn es hierfür keine feste zeitliche Begrenzung gibt), falls die Datenschutzverletzung vermutlich mit einem hohen Risiko für ihre Rechte und Freiheiten verbunden ist. Es gibt eine Reihe begrenzter Ausnahmen in Bezug auf die Meldepflicht an eine Aufsichtsbehörde und die Benachrichtigung der Betroffenen. Hierzu sollten sich Unternehmen rechtlich beraten lassen.

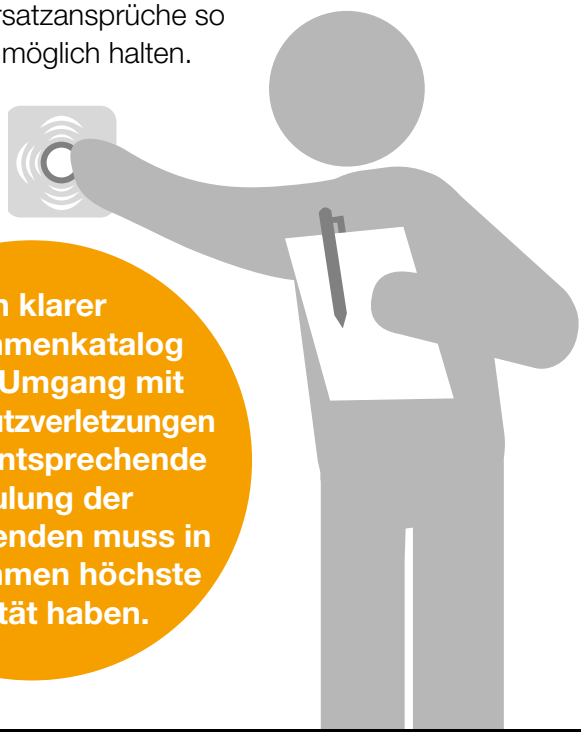
Die Meldung von Datenschutzverletzungen verkompliziert sich durch folgende Punkte:

- Die Tatsache, dass es in bestimmten Ländern (einschließlich Österreich, Deutschland und der Niederlande) bereits eigene Meldepflichten für Datenschutzverletzungen gibt
- Die Tatsache, dass Meldungen von Datenschutzverletzungen im Rahmen anderer Verordnungen und Vorschriften erforderlich sein können, speziell im Finanz- oder Gesundheitswesen
- Die Tatsache, dass weitere separate Gesetze in der EU in Übereinstimmung mit der EU-Richtlinie zur Cyber-Sicherheit implementiert werden sollen



Wie sieht es mit Haftung und Schadenersatz aus?

Generell gilt, dass jeder, dem aufgrund eines Verstoßes gegen die neue Verordnung ein Schaden entstanden ist, gegenüber den Personen, welche die betreffenden personenbezogenen Daten kontrollieren oder verarbeiten, ein Anrecht auf Ersatz des entstandenen Schadens hat, vorbehaltlich bestimmter Ausnahmen. Aufgrund des zusätzlichen Risikos, das bei Verstößen gegen die neue Verordnung speziell bei einer Datenschutzverletzung nun bestehen kann, müssen Unternehmen das Potenzial für Schadenersatzansprüche so gering wie möglich halten.



Ein klarer Maßnahmenkatalog für den Umgang mit Datenschutzverletzungen und die entsprechende Schulung der Mitarbeitenden muss in Unternehmen höchste Priorität haben.

Müssen irgendwelche Bewertungen bezüglich der Auswirkungen auf den Datenschutz durchgeführt werden?

Ja. Im Rahmen der neuen Verordnung werden diese Bewertungen Datenschutz-Folgeabschätzungen genannt. Wo die Verarbeitung von Daten (speziell mittels neuer Technologien) vermutlich mit einem hohen Risiko für die Rechte und Freiheiten von Personen verbunden ist, muss eine Abschätzung der Folgen durchgeführt werden, die die geplanten Verarbeitungsschritte auf die Sicherheit der personenbezogenen Daten haben – und zwar vor der Verarbeitung. Eine Datenschutzaufsichtsbehörde ist (ebenfalls vor der Verarbeitung) zu konsultieren, falls eine Folgeabschätzung darauf hinweist, dass die Verarbeitung ohne Maßnahmen zur Minderung des Risikos mit einem hohen Risiko verbunden wäre.

Datenschutz-Folgeabschätzungen werden in Zukunft vermutlich die Regel sein und sich als sehr nützliches Hilfsmittel im Umgang mit Datenschutzrisiken erweisen, unter anderem bei der Abschätzung der Datensicherheitsrisiken und der Abwägung der Risiken bei der Verarbeitung personenbezogener Daten, beispielsweise durch versehentliche oder ungesetzliche Vernichtung.

Gibt es auch Änderungen in Bezug auf die Datenübermittlung an Drittländer?

Nicht wirklich. Spezielle bestehende Vorschriften bezüglich der Übermittlung von Daten aus EU-Mitgliedstaaten an Drittländer (einschließlich der USA) bleiben im Rahmen der neuen DSGVO in Kraft, einschließlich der Anforderung, dass solche Datenübermittlungen nur stattfinden dürfen, wenn die jeweiligen Drittländer einen angemessenen Datenschutz sicherstellen. Allerdings werden die Vorschriften teilweise etwas detaillierter ausgeführt. Dies ist ein komplizierter Themenkomplex, der auch noch im Rahmen der bestehenden Datenschutzverordnung in Entwicklung ist. Wir empfehlen Ihnen daher, Ihre Rechtsabteilung zu Rate zu ziehen.

Wo kann ich weitere Informationen finden?

Die neue Verordnung ist auf der Website der Europäischen Kommission **zu finden**

Was sollte ich als Nächstes tun?

Für die mit der Einhaltung der DSGVO verbundenen Vorbereitungen sollten Sie ein Budget erstellen und Ressourcen einplanen (einschließlich IT). Berücksichtigen Sie bei Ihrer Planungszeit auch die notwendige Anpassung. Die folgenden zehn Punkte sollten Sie vorrangig behandeln:

1. **Setzen Sie einen Prozess für die Datenschutz-Folgeabschätzung in Kraft – kartografieren Sie Ihre Daten und bestimmen Sie die Risikobereiche**
2. **Unterziehen Sie Ihre Lieferantenverträge einer gründlichen Überprüfung – Sie werden die Hilfe Ihrer Lieferanten benötigen, speziell wenn es um die rasche Meldung von Sicherheitsverletzungen geht, deshalb sollten Sie sicherstellen, dass Sie das vertragliche Recht haben, darauf zu bestehen**
3. **Aktualisieren Sie Ihre Systeme und Materialien und arbeiten Sie detaillierte neue Dokumentationen und Aufzeichnungen aus, die Sie den Aufsichtsbehörden bei Bedarf vorlegen können**
4. **Prüfen Sie die wesentlichen praktischen Gesichtspunkte einschließlich der Aufbewahrung der Daten für alle vom Unternehmen verwendeten Daten**
5. **Gewährleisten Sie, dass entsprechende Maßnahmen in Kraft sind, um alle nicht benötigten Daten sicher zu vernichten**
6. **Achten Sie darauf, dass neue Gesichtspunkte wie die ausdrückliche Einwilligung, das Recht auf Vergessenwerden, das Recht auf Datenübertragbarkeit und das Widerspruchsrecht in alle Richtlinien und Verfahren aufgenommen werden**
7. **Richten Sie ein Verfahren für die Benachrichtigung bei Datenschutzverletzungen ein, einschließlich Kapazitäten für die Erkennung und Reaktion, und proben Sie die Abläufe wie bei einer Feuerschutzübung**
8. **Überlegen Sie, einen Datenschutzbeauftragten zu ernennen**
9. **Schulung, Schulung, Schulung – Schulen Sie Ihren Mitarbeiterstab in allen oben aufgeführten Punkten (Datenschutzaufsichtsbehörden achten besonders darauf)**
10. **Führen Sie regelmäßige Compliancеprüfungen durch, um Probleme zu erkennen und zu beheben**

Dank an unsere Experten

Jonathan Armstrong und **André Bywater** von **Cordery Compliance** waren uns mit ihrer fundierten Erfahrung in DSGVO-Belangen bei der Ausarbeitung dieses Whitepapers behilflich.

www.corderycompliance.com

Jonathan Armstrong
Cordery
Lexis House
30 Farringdon Street,
London, EC4A 4HH
+44 (0)207 075 1784
jonathan.armstrong@corderycompliance.com

André Bywater
Cordery
Lexis House
30 Farringdon Street
London, EC4A 4HH
+44 (0)207 075 1785
andre.bywater@corderycompliance.com

Über Fellowes: Fellowes ist ein weltweiter Hersteller und Vermarkter von Büromaschinen, Archivlösungen und Arbeitsplatzzubehör. Unsere Produkte wurden entwickelt um **Qualität, Effizienz** und **Produktivität am Arbeitsplatz** zu steigern.

www.fellowes.com

Fellowes GmbH
Fliegerstr. 1
30179 Hannover
cs-germany@fellowes.com

Cordery® Legal.Compliance

Fellowes WORK BETTER™