Frank Haug

Zert. Datenschutzbeauftragter (TÜV)
Consultant für Datenschutz und Informationssicherheit

EU-Datenschutz-Grundverordnung

November | 2016

Wichtige Datenschutzinformationen für Ihr Unternehmen

Inhalte | Datenschutzinformationen | November 2016

Inhaltsverzeichnis

Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Frank Haug

Liebe Leserin, lieber Leser,

am 14. April 2016 wurde durch das EU-Parlament die EU-Datenschutz-Grundverordnung (EU-DSGVO) beschlossen, die zukünftig den Umgang von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen einheitlich für die gesamte europäische Union regeln wird.

Sie löst mit einer zweijährigen Übergangsfrist alle vorherigen Datenschutzgesetze ab und ist ab 25. Mai 2018 für alle Unternehmen in der EU bindend.

Da es in der EU-Datenschutz-Grundverordnung viele neuen Richtlinien und Änderungen gibt, die teilweise deutlich über das Bundesdatenschutzgesetz hinausgehen, bzw. von diesem abweichen, muss sich jedes Unternehmen in Deutschland kurzfristig mit diesem Thema auseinandersetzen.

Grund genug, um uns in dieser Ausgabe der neuen EU-Datenschutz-Grundverordnung (EU-DSGVO) zu widmen. Nutzen Sie diese Informationen und bereiten Sie sich schon jetzt für einen optimalen und reibungslosen Übergang vor, so dass Sie dem 25. Mai 2018 gelassen entgegensehen können.

Sollten Sie darüber hinaus weitere Informationen benötigen oder eine ausführliche Beratung in Anspruch nehmen wollen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung. Sie erreichen uns unter der Telefonnummer (09421) 1834 - 03 oder per E-Mail an kontakt@dsb-fh.de.

Mit besten Grüßen

Frank Haug
Zert. Datenschutzbeauftragter (TÜV)
Consultant für Datenschutz und Informationssicherheit

Grundverordnung | Darauf müssen Unternehmen achten

Neue Regelungen

Neue datenschutzrechtliche Regelungen definieren einen europaweiten Standard für den Umgang mit personenbezogenen Daten. Doch was müssen Unternehmen dabei beachten?

Nachdem die EU-Datenschutzgrundverordnung (kurz: EU-DSGVO) verabschiedet wurde, profitieren die Bürger der Mitgliedsstaaten der Europäischen Union (EU) künftig von einem einheitlichen Schutzniveau. Sie sind mehr denn je vor der Speicherung und Weitergabe von Daten durch international operierende Unternehmen geschützt. Gleichbedeutend kommen aber auch Aufgaben auf alle Unternehmen zu, um auch zukünftig datenschutzkonform aufgestellt zu sein.

Die EU-DSGVO tritt am 25. Mai 2018 in Kraft und definiert den Mindeststandard, wie mit der Verarbeitung personenbezogener Daten innerhalb der EU umgegangen wird. Vereinfacht gesagt, müssen die Regelungen bis zu diesem Datum umgesetzt sein, da wir uns bereits in der Übergangsfrist befinden. Die meisten Mitgliedsstaaten werden wesentlich mehr Vorgaben umsetzen müssen als die Bundesrepublik, doch auch Unternehmen in Deutschland sollten sich früh genug der Herausforderung stellen und zeitnah mit der Umsetzung beginnen.

Zu den wichtigsten Neuerungen gehören:

- ✓ Bestimmte Meldepflichten
- ✓ „Recht auf Vergessenwerden“
- ✓ Datenschutz-Folgenabschätzung
- ✓ Erweiterte Dokumentationspflichten
- ✓ Empfindlichere Bußgelder

Meldepflichten

Unter den Meldepflichten versteht man unter Anderem, dass betroffene Personen und die Aufsichtsbehörde binnen 72 Stunden nach einem Datenschutzverstoß darüber informiert werden müssen, wenn ihre persönlichen Daten kompromittiert wurden und dies eine ernsthafte Bedrohung ihrer Rechte und Freiheiten darstellt.

„Recht auf Vergessenwerden“

Wenn betroffene Personen nicht möchten, dass ihre Daten weiter verarbeitet werden und es keine gesetzliche Grundlage für deren Speicherung gibt, müssen die Daten gelöscht werden.

Dieses kennt man bereits aus dem Bundesdatenschutzgesetz (BDSG). Die EU-DSGVO geht jetzt aber noch einen Schritt weiter, so dass auch Dritte, die die Daten verarbeiten, über den Löschwunsch des Betroffenen informiert werden müssen. Dabei sind im Rahmen des wirtschaftlich und technisch Machbaren, entsprechende Maßnahmen zu treffen, um auch diese Verarbeiter darüber zu informieren.

Um diese Vorgaben rechtskonform zu erfüllen ist es sehr wichtig, auch die Löschkonzepte Ihres Unternehmens genau zu analysieren – nicht nur zur Vorbereitung auf die EU-DSGVO, sondern auch um bereits bestehendes Datenschutzrecht einzuhalten.

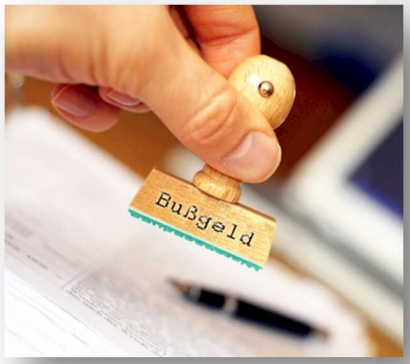
Datenschutz-Folgenabschätzung

Durch die Datenschutzgrundverordnung wird jetzt neu auch die Datenschutz-Folgenabschätzung eingeführt. Diese ist in folgenden Fällen vorzunehmen:

- ✓ bei einer systematischen und umfassenden Bewertung persönlicher Aspekte, natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet […];
- ✓ umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten;
- ✓ systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Wichtig: Unternehmen sollten sich frühzeitig mit dieser Thematik auseinandersetzen, da bei Feststellung eines hohen Risikos eine Konsultationspflicht gegenüber den Aufsichtsbehörden besteht!

Grundverordnung | Wichtige Neuerungen



Erweiterte Dokumentationspflichten

Nicht nur das Bundesdatenschutzgesetz, sondern auch die vor uns liegende EU-DSGVO betont die Wichtigkeit der Dokumentation. So ist zum Beispiel eine lückenlose Dokumentation

- ✓ der „Verletzungen des Schutzes personenbezogener Daten“ inklusive deren Auswirkungen und Abhilfemaßnahmen,
- ✓ dem „Verzeichnis von Verarbeitungstätigkeiten“,
- ✓ und von Nachweisen von Datenschutzmaßnahmen im Falle einer Auftragsverarbeitung

nötig, um zukünftig die gesetzlichen Anforderungen erfüllen zu können. Eine frühzeitige Prüfung vorhandener Dokumentation ist also Pflicht.

Empfindlichere Bußgelder

Die Sanktionen für Datenschutzverstöße werden mit Einführung der EU-DSGVO drastisch erhöht. Waren Bußgelder in der aufsichtsbehördlichen Praxis eher die Ausnahme, können diese zukünftig wesentlich häufiger verhängt werden.

Im BDSG sind Bußgelder bis zu 300.000 Euro vorgesehen, bei wirtschaftlichem Vorteil in Einzelfällen auch schon mal mehr. Zukünftig können Bußgelder bis zu 20 Millionen Euro bzw. 4% des weltweiten Jahresumsatzes gegen Unternehmen verhängt werden. Die Berechnung des Umsatzes knüpft dabei an den Umsatz der gesamten Unternehmensgruppe, nicht nur allein an der juristischen Person, die den Datenschutzverstoß zu verantworten hat. Die konkrete Bußgeldhöhe wird von den Umständen des jeweiligen Einzelfalls abhängen und kann auch deutlich unter den Höchstgrenzen liegen.

Neu in der Gesetzgebung der EU-DSGVO sind der Direktanspruch des Betroffenen auch gegen den Auftragsverarbeiten und die Beweislastumkehr. So muss zukünftig nachgewiesen werden, dass das Unternehmen alle nötigen Schritte eingeleitet hat. Dies könnte zu vermehrten Beschwerden und Klagen führen. Unternehmen sollten sich daher darauf einstellen, indem Sie ihre datenschutzrechtlichen Prozesse gut dokumentieren, um sich gegen unbegründete Beschwerden ohne erhöhten Aufwand verteidigen zu können.

Was Cloud-Nutzer beachten sollten

Cloud-Nutzer müssen die Datenschutzvorgaben der EU-DSGVO genau kennen und implementieren, da auch hier einige Neuerungen hinzugekommen sind.

Cloud-Nutzer werden in der Datenschutz-Grundverordnung auf viele bekannte Datenschutzvorgaben stoßen. So müssen beispielsweise schon heute rechtliche Grundlagen für die Verarbeitung vorliegen, die Datensparsamkeit beachtet und eine Reihe von Informationsrechten berücksichtigt werden. Ebenfalls von großer Bedeutung ist die Datenabsicherung in der Cloud. Hatten die Cloud-Nutzer bisher große Schwierigkeiten das angemessene Schutzniveau (regelmäßig) zu überprüfen, sieht die EU-DSGVO hier neue Instrumente vor.

So können Cloud-Anbieter zukünftig durch „genehmigte Verhaltensregeln“ oder einer „Zertifizierung durch eine akkreditierte Stelle“, die technischen und organisatorischen Maßnahmen nachweisen. Die Verhaltensregeln müssen durch die Aufsichtsbehörden genehmigt und veröffentlicht werden.

Folgend finden Sie noch weitere Aspekte, die ebenfalls zu beachten sind:

- ✓ Cloud-Migration muss möglich sein – „Datenübertragbarkeit“
- ✓ EU-Datenschutz auch für ausländische Anbieter – „Marktortprinzip“
- ✓ Grenzüberschreitender Datenverkehr und Zuständigkeit der Aufsichtsbehörde – „One-Stop-Shop“

Bereits diese Aspekte zeigen auf, dass die Cloud-Services, die bereits genutzt oder zukünftig genutzt werden sollen, einer genaueren Untersuchung zu unterziehen sind. Besonders wichtig ist die Einhaltung der rechtlichen Grundlagen bei grenzüberschreitendem Datenverkehr.

Grundverordnung | Auftragsdatenverarbeitung

Welche Änderungen haben Unternehmen zu erwarten?

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch einen Auftragnehmer unter Weisung der verantwortlichen Stelle wird als Auftrags-datenverarbeitung bezeichnet und muss bereits im heutigem Datenschutzrecht vertraglich geregelt sein. Doch wie sieht es zukünftig aus?

Was zuerst auffällt, sind die sprachlichen Änderungen, die mit der EU-DSGVO eingeführt wurden. Zukünftig spricht man von „*Auftragsverarbeiter*“ und „*den für die Verarbeitung Verantwortlichen*“. Der Vertrag zwischen den Parteien orientiert sich am Vertrag zur Auftragsdatenverarbeitung nach dem BDSG.

Größere Änderungen kommen auf die Auftragsverarbeiter zu. So sind beispielsweise folgende Punkte zu beachten:

- ✓ Der Auftragsverarbeiter muss ein Verzeichnis über die Verarbeitung führen
- ✓ Die bekannten Meldepflichten bestehen fort
- ✓ Für die Verarbeitung Verantwortliche und Auftragsverarbeiter haften gleichermaßen bei Verstößen gegenüber dem Betroffenen

Neu ist, dass eine Auftragsverarbeitung auch außerhalb der Europäischen Union möglich ist, was die Datenverarbeitung (z.B. durch einen Cloud-Anbieter) zusätzlich vertraglich regelt.

Auch wenn auf deutsche Unternehmen, die eine Datenverarbeitung im Auftrag nutzen, nur wenige Änderungen zukommen, sollten die bestehenden Verträge geprüft, gegeben falls Änderungen vorgenommen und neue Verträge der sich ändernden Gesetzeslage angepasst werden.

Auftragsverarbeiter hingegen sollten sich zeitnah auf die kommenden Regelungen einstellen, um potentielle Bußgelder zu vermeiden.

Bleiben bestehende Regelungen für internationalen Datentransfer wirksam?

Sofern eine Rechtsgrundlage für die generelle Datenübermittlung existiert, kann mit den zur Verfügung stehenden Instrumenten die Übermittlung auch in einen Drittstaat erfolgen. Diese sind:

- ✓ Binding Corporate Rules (BCR), verbindliche, selbstauferlegte Unternehmensvorschriften zum Umgang mit personenbezogenen Daten
- ✓ EU-Standardverträge, von der EU-Kommission vorgegebene Modelklauseln, deren Inhalt nicht abgeändert werden darf.

Falls eine Einwilligung des Betroffenen vorliegt oder die geltenden Regelungen zur Erfüllung eines Vertrages notwendig sind, können auch bestehende Datenschutz-Richtlinien für den Datentransfer angewandt werden.

Um sich auf die obengenannten Regelungen der Datenschutz-Grundverordnung vorzubereiten, sollten Unternehmen folgende Maßnahmen ergreifen:

- ✓ Analyse der bestehenden Datenflüsse in Drittstaaten.
- ✓ Identifizierung der bestehenden Rechtsgrundlagen bzw. Mechanismen zur Herstellung eines angemessenen Datenschutzniveaus.
- ✓ Im Anschluss an die Feststellung der Datenflüsse und deren Bedeutung und Funktion für das Unternehmen sollte evaluiert werden, welcher Transfermechanismus für das eigene Unternehmen die praktikabelste Lösung ist.

Die EU-DSGVO schafft zwar – im Vergleich zur geltenden Gesetzgebung – viele weitere Vereinheitlichungen im EU-Datenschutzrecht, die insbesondere den Dialog zu Datenschutzthemen mit Vertragspartnern in und jenseits der EU vereinfachen werden, jedoch auch zahlreiche Spielräume für nationale Regelungen in der DSGVO. Diese müssen also im Einzelfall betrachtet werden, was einen erheblichen Mehraufwand bedeuten kann. Zudem ist zurzeit noch nicht abschätzbar, welche Sondervorschriften die Öffnungsklauseln der einzelnen Mitgliedsstaaten mit sich bringen.

Wie kann ich mich auf die Änderungen durch die Grundverordnung vorbereiten?

Unternehmen sollten angesichts der Änderungen, die auf sie zukommen, das bestehende Datenschutzmanagement-System genauer unter die Lupe nehmen. Dabei sind die folgenden Anmerkungen erste Anhaltspunkte, sich den Herausforderungen zu stellen.

Bestandsaufnahme

Für ein erfolgreiches Datenschutzmanagement-System ist eine lückenlose Dokumentation unumgänglich. So sollten sich Unternehmen schon jetzt mit folgenden Fragestellungen konfrontieren:

- ✓ Wie werden Daten in meinem Unternehmen verarbeitet?
- ✓ Besitze ich ein umfassendes Verfahrensverzeichnis?
- ✓ Habe ich einen Überblick über meine Auftragsdatenverarbeitung und übermittle ich personenbezogene Daten in ein „*Drittland*“?
- ✓ Liegen für die Datenübermittlung Rechtsgrundlagen vor?
- ✓ Sind meine Datenschutzerklärungen und Einwilligungen vollständig und dokumentiert?
- ✓ Sind die datenschutzrechtlichen Prozesse nachvollziehbar dokumentiert?

Mit dieser Bestandsaufnahme sollte sofort begonnen werden, um ausreichend Zeit für nötige Änderungen zu besitzen.

Änderungsbedarf

Liegen die Dokumentationen vor, sollte mit der Ermittlung des Änderungsbedarfs begonnen und die benötigten Schritte eingeleitet werden. Je nach vorliegender Dokumentation, sollte dies bis spätestens Dezember 2017 abgeschlossen sein um noch genügend zeitlichen Spielraum zu besitzen, fehlende Dokumentation zu erstellen oder datenschutzrechtliche Prozesse an die neue EU-DSGVO anzulehnen. Erfahrungsgemäß müssen Einwilligungen angepasst und die Verfahrensverzeichnisse meist vor allem bei der Auftragsdatenverarbeitung überarbeitet werden.

Neue Prozesse verankern

Mit der EU-DSGVO werden eine Reihe von Konzepten und entsprechende Verpflichtungen eingeführt, die so bisher noch nicht vorhanden waren. Das sind zum Beispiel:

- ✓ Datenschutz-Folgenabschätzung (Privacy Impact Assessment, PIA)
- ✓ Datenübertragbarkeit
- ✓ „Recht auf Vergessenwerden“
- ✓ Meldepflichten

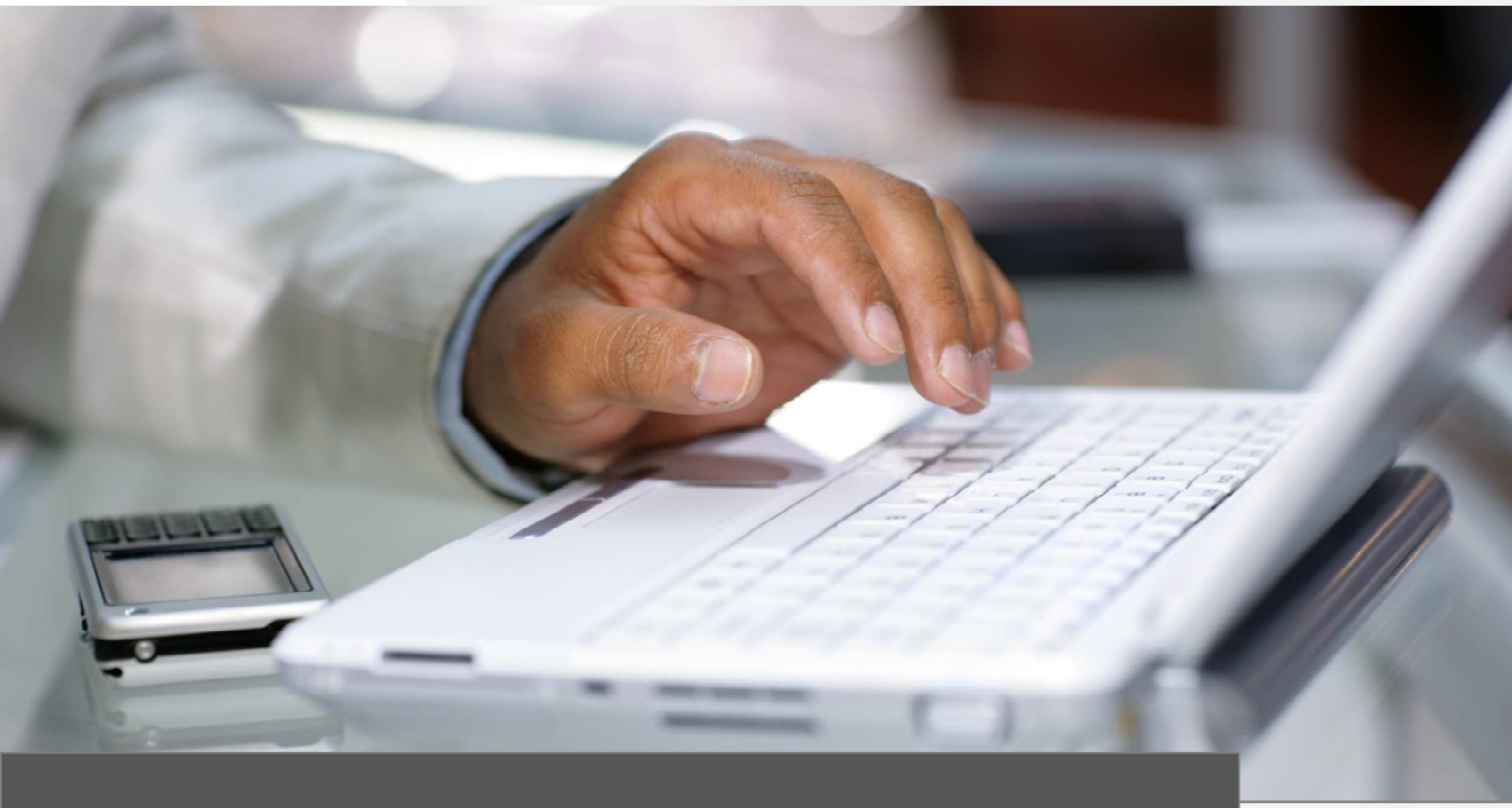
Diese Prozesse müssen in den meisten Unternehmen komplett neu erstellt und in das vorhandene Datenschutzmanagement-System eingepflegt werden. Bis Mai 2018 sollten diese dann in die gängige Praxis übergegangen sein.

Fazit: Die EU-DSGVO bringt gegenüber den bisherigen datenschutzrechtlichen Vorschriften erhebliche Veränderungen mit sich und Unternehmen müssen viele zusätzliche Anforderungen erfüllen. Fast jede neue Regelung ist zudem bußgeldbewehrt. Unternehmen sind daher gut beraten, mit den notwendigen Veränderungen sehr zeitnah zu beginnen. Dies erfordert vor allem die Anpassung von Arbeitsabläufen, IT-Systemen, Dokumentationen und Strukturen der Datenverarbeitung.

Frank Haug

Zert. Datenschutzbeauftragter (TÜV)
Consultant für Datenschutz unf Informationssicherheit

November | 2016



Impressum

Frank Haug
Zert. Datenschutzbeauftragter (TÜV)
Consultant für Datenschutz und Informationssicherheit

Emanuel-Schikaneder-Str. 22
94315 Straubing
Tel.: +49 (9421) 1834 - 03
Fax: +49 (9421) 1834 - 26
Web: www.dsb-fh.de

Redaktion:
Frank Haug

Bildnachweise:
Diese Datenschutzbroschüre wurde in unserem Auftrag von der Firma ITKservice GmbH & Co. KG, Fuchsstädter Weg 2, 97491 Aidhausen erstellt. Alle in diesem Dokument dargestellten Bilder wurden