ENDPOINT
ENCRYPTION

Quick Guide zur EU-Datenschutzgrundverordnung

ENJOY SAFER TECHNOLOGY™

Die Datenschutzgrundverordnung (DSGVO) ersetzt die Datenschutzrichtlinie 95/46/EG aus dem Jahr 1995. Ziel ist es, den Grundrechtsschutz und Datenschutz für EU-Bürger zu stärken. Zudem soll das bislang bestehende Sammelsurium aus 28 verschiedenen nationalen Gesetzen durch ein europaweit einheitlich geregeltes Datenschutzrecht abgelöst werden. Die Verordnung wird ab dem 25. Mai 2018 Anwendung finden.

Was sind die wesentlichen Änderungen?[1]

- Unternehmen und Organisationen müssen den nationalen Aufsichtsbehörden alle Datenschutzverstöße melden, durch die ein Risiko für den betroffenen Bürger entstanden ist. Zudem muss die betroffene Person so rasch wie möglich über alle mit hohem Risiko behafteten Verstöße informiert werden, damit er entsprechend reagieren kann.
- Stärkere Durchsetzung der Vorschriften: Datenschutzbehörden können Geldstrafen gegen Unternehmen verhängen, die gegen EU-Vorschriften verstoßen. Diese Geldstrafen können bis zu 4 % des weltweiten Jahresumsatzes eines Unternehmens ausmachen. Bußgelder sind nicht zwingend und müssen einzelfallangemessen sowie verhältnismäßig sein. Allerdings sollen sie ausdrücklich auch abschreckend wirken.
- Ein Kontinent, ein Recht: ein einheitliches europäisches Datenschutzrecht ersetzt die verschiedenen Gesetze der Mitgliedstaaten. Unternehmen müssen sich nur noch mit einem einzigen und nicht mit 28 verschiedenen Gesetzen auseinandersetzen. Damit lassen sich jährlich schätzungsweise 2,3 Mrd. EUR einsparen.
- Organisationen müssen die nationalen Behörden bei schweren Datenschutzverletzungen unverzüglich informieren (binnen 72 Stunden).
- Die Regelungen der DSGVO gelten auch für Unternehmen, die keine Niederlassung in der EU haben, aber EU-Bürgern Waren- und Dienstleistungen (einschließlich kostenfreier Waren- und Dienstleistungen) anbieten oder deren Verhalten überwachen.
- Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen sind nunmehr wesentliche Elemente der EU-Datenschutzvorschriften. Datenschutzgarantien werden bereits frühzeitig in die Entwicklung von Erzeugnissen und Dienstleistungen integriert und datenschutzfreundliche Voreinstellungen werden beispielsweise in sozialen Netzwerken oder Mobilen Apps zur Norm.

Mit dem gestärkten Datenschutz werden Unternehmen in die Pflicht genommen, personenbezogene Daten angemessen zu schützen. Diese werden definiert als:

„alle Informationen über eine bestimmte oder bestimmbare natürliche Person (nachstehend „betroffene Person" genannt); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;"[2]

Diese weite Definition personenbezogener Daten deckt auch Informationen ab, die lediglich indirekt auf Kunden, Konsumenten, Mitarbeiter, Studenten oder Schüler verweisen sowie jegliche andere Daten über Individuen.

Wie steht die EU zum Schutz von Daten?

In Artikel 32 zur Sicherheit der Verarbeitung heißt es[3]:

> *1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:*
>
> *a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*
>
> *b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*
>
> *c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*

1 Europäische Kommission - Factsheet: http://europa.eu/rapid/press-release_MEMO-15-6385_de.pdf

2 Verordnung (EG) Nr. 45/2001: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:de:PDF

3 DSGVO: http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32016R0679

> *d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*

Mithilfe von Verschlüsselung werden Daten ganz unkompliziert und sicher entsprechend Artikel 32 der DSGVO geschützt. Mit dieser Technologie bleiben Informationen selbst bei Verlust oder Diebstahl eines Geräts sicher. Darüber hinaus betont die DSGVO die Relevanz von effektiven Notfallplänen, Passwortwiederherstellungen und Schlüsselmanagement-Systemen.

Artikel 30 der Verordnung[3] fordert ein Verzeichnis von Verarbeitungstätigkeiten, das eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 beinhaltet. Organisationen müssen dokumentieren und beweisen, dass die Systeme sicher und verschlüsselte Daten nach einem technischen Vorfall wiederherstellbar sind.

Welche Regelungen beinhaltet die Meldepflicht?

Artikel 33[3] fordert die Meldung von Verletzungen des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden. Erfolgt die Meldung erst nach diesem geforderten Zeitraum, muss die Verzögerung begründet werden.

Artikel 34[3] bezieht sich auf die Benachrichtigung der Verletzung des Schutzes personenbezogener Daten gegenüber der betroffenen Person und fordert:

> *1. Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.*

Allerdings heißt es weiter:

> *3. Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:*
>
> *a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung,*
>
> *b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht,*
>
> *c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.*

Studien belegen, dass je früher ein Datenverlust gemeldet wird, die Folgen für die betreffende Organisation umso schlimmer sind. Verschlüsselung bietet ein sicheres Netz, um solche Schäden für den Ruf des Unternehmens zu verhindern.

Inwiefern hat die DSGVO abschreckende Wirkung?

In Artikel 83 zu den allgemeinen Bedingungen für die Verhängung von Geldbußen heißt es in Absatz 4[4]:

> *4. Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:*
>
> *a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43;*

Mit diesen Geldbußen werden Verletzungen der Meldepflicht im Sinne von Artikel 33 und 34 abgedeckt. In Artikel 83 Absatz 5 heißt es allerdings weiter:

> *5. Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:*
>
> *a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;*

4 DSGVO: http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32016R0679

In Artikel 5 über die Grundsätze für die Verarbeitung personenbezogener Daten steht unter anderem:

> *1. Personenbezogene Daten müssen*
> *f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit");*

Diese Strafen sollen ausdrücklich „abschreckend" sein. Angesichts der Tatsache, dass sie in weniger als zwei Jahren auch angewendet werden, sollten Unternehmen schnellstmöglich entsprechende Vorkehrungen treffen.

Welche Maßnahmen sollten Unternehmen ergreifen?

Die Verordnung fordert von Organisationen jeder Größenordnung die Implementierung neuer Prozesse und Strategien. Für einige bedeutet das, dass neue Prozesse definiert, Handbücher umgeschrieben, Mitarbeiter geschult und Systeme aktualisiert werden müssen. Hinzu kommen praktische Maßnahmen wie die Einführung von Verschlüsselungstechnologien zum Schutz sensibler Daten.

Ein verlorener oder gestohlener Laptop muss nicht zwangsläufig ein hohes Bußgeld nach sich ziehen, sofern er sicher verschlüsselt ist. Mit ESET Endpoint Encryption können Unternehmen all ihre Geräte und Daten – Laptops, Wechselmedien, E-Mails und Dateien – zuverlässig verschlüsseln. Unsere Produktpalette deckt alle Windows-Plattformen von XP bis Windows 10 sowie iOS der Version 7 und neuer ab. Unsere Software basiert auf einem FIPS 140-2-validierten kryptografischen Subsystem (Level 1) und unser Schlüssel-Verwaltungssystem sowie der Management-Server sind international patentiert.

Wie bereits Artikel 5 verdeutlicht, besteht einer der Grundsätze der DSGVO in der Gewährleistung eines angemessenen Schutzes personenbezogener Daten. Artikel 32 zur Sicherheit der Verarbeitung nennt die Verschlüsselung als dafür geeignete technische Maßnahme. Beim Einsatz von Verschlüsselungslösungen ist auch darauf zu achten, dass die Daten sowie das System nach einem Vorfall sicher wiederhergestellt werden können.

ESET Endpoint Encryption bietet Unternehmen einen unkomplizierten und effektiven Weg, diesen Anforderungen gerecht zu werden:

Ziel	ESET Endpoint Encryption
Gespeicherte Daten innerhalb der Organisation schützen	Alle kommerziellen Versionen von ESET Endpoint Encryption Encryption by ESET ermöglichen standardmäßig die Verschlüsselung von Dateien, Ordnern und Wechselmedien.
Daten bei der Übertragung schützen	Mit ESET Endpoint Encryption Pro lassen sich ganze Festplatten sowie Wechselmedien wie USB-Geräte und optische Datenträger verschlüsseln. So bleiben Ihre Daten auch unterwegs sicher.
Daten über das Unternehmensnetzwerk hinaus schützen	Kommerzielle ESET Endpoint Encryption Lizenzen ermöglichen eine zusätzliche Installation auf privaten PCs. Darüber hinaus bietet ESET Endpoint Encryption Go eine mobile Lösung zur Ver- und Entschlüsselung von USB-Geräten.
Die Übermittlung von Daten zwischen zwei Speicherorten absichern	Alle ESET Endpoint Encryption Versionen beinhalten ein Outlook-Plugin, mit dem Sie E-Mails und Anhänge problemlos verschlüsseln können. Die Verschlüsselung der Zwischenablage funktioniert mit allen E-Mail-Programmen, einschließlich Webmail.
Den Zugriff auf bestimmte Daten blockieren / einschränken	Dank der patentierten Key-Sharing-Technologie wird selbst bei teamübergreifenden und komplexen Arbeitsgruppen ein unkomplizierter Datenaustausch gewährleistet.
Den sicheren Datenzugriff auf Anfrage gestatten	Der ESET Endpoint Encryption Enterprise Server ermöglicht die zentralisierte Nutzer-Verwaltung über eine sichere Internetverbindung. Zudem lassen sich Schlüssel zentral hinzufügen und entfernen.
Sichere Speicherung personenbezogener Daten gewährleisten	ESET Endpoint Encryption ist FIPS 140-2-validiert und nutzt zuverlässige und sichere, dem Industriestandard entsprechende Verschlüsselungsalgorithmen und -methoden.
Sichere Löschung redundanter Daten gewährleisten	Mit dem ESET Endpoint Encryption Shredder Tool werden Daten gemäß DoD-5220.22-M-Standard sicher gelöscht und können nicht wiederhergestellt werden.

Artikelnummer: M_Print2017_07 | Stand: Januar 2018