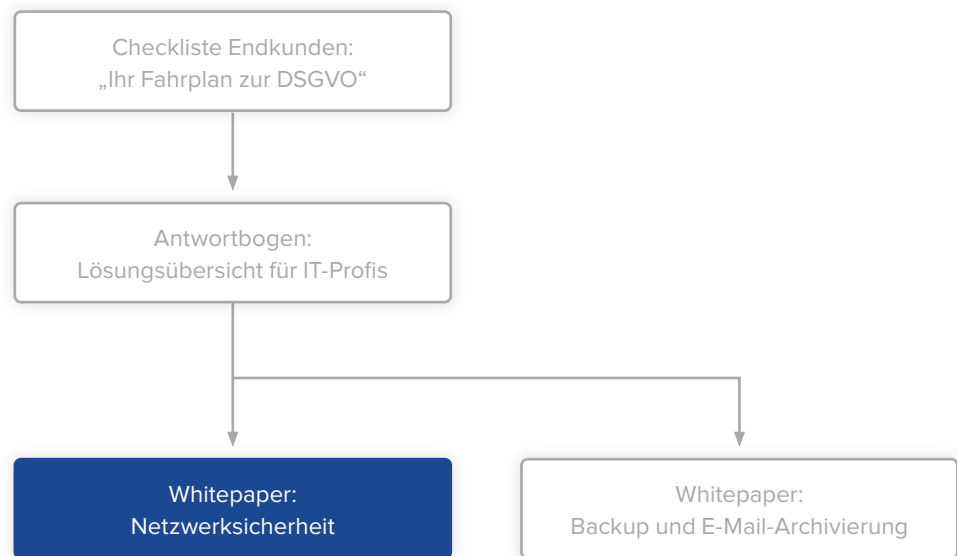


Themenserie DSGVO: Netzwerksicherheit

Die Themenserie zur DSGVO im Überblick

Hier finden Sie alle unsere Materialien zur DSGVO zu einem Workflow sortiert, damit Sie Ihre Kunden bestmöglich auf die DSGVO vorbereiten und proaktiv die Projektplanung beginnen können:





Vorwort

Am 25. Mai 2018 trat die EU-Datenschutz-Grundverordnung (DSGVO) vollumfänglich in Kraft. Verstöße gegen die DSGVO können empfindlich hohe Strafen nach sich ziehen – damit stehen Ihre Kunden unter Zugzwang, den Umgang mit personenbezogenen Daten auf den Prüfstand zu stellen und Prozesse rechtlich neu zu ordnen. Das betrifft auch die gesamte IT-Infrastruktur, von Mechanismen der Netzwerksicherheit über System-Management bis hin zu Backup- und E-Mail-Archivierungssystemen.

Inhalt

1.	Einleitung	5
2.	Artikel 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung	6
3.	Maßnahmen zum Datenschutz: die technische Umsetzung	8
3.1	ESET – Sicherheit auf allen Ebenen	10
4.	IT-Security und Datenschutz: Was sind Ihre nächsten Schritte?	11

1. Einleitung

Wir möchten Sie als IT-Profi in der Argumentation und Projektplanung bei Ihren Kunden unterstützen. Daher informieren wir Sie in unserer Whitepaper-Serie zu den für Sie relevantesten – weil technisch umsetzbaren – Artikeln der [DSGVO](#). Der zweite Teil unserer Serie beschäftigt sich mit dem Artikel 25 “Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen”¹ und wie IT-Security-Lösungen sich in diesem Rahmenwerk bewegen.

Als IT-Dienstleister stehen Sie dabei vor der Herausforderung, die Möglichkeiten zur Umsetzung der DSGVO zu identifizieren, sie mit den vorhandenen Gegebenheiten in Einklang zu bringen und auf dieser Basis bei Ihren Kunden eine geeignete Sicherheitsstrategie anzubringen. Erschwerend kommt hinzu, dass die Datenschutz-Grundverordnung in ihrer Komplexität nicht mit einer einzigen Lösung, sondern nur aus verschiedenen Ansatzpunkten heraus vollumfänglich umgesetzt werden kann. So können auch technische Maßnahmen nur ein Baustein zur DSGVO-Konformität sein, neben organisatorischen und personellen Prozessen.

In diesem Whitepaper erfahren Sie, welche gesetzlichen Rahmenkriterien beim Thema IT-Security zu bedenken sind und welche Lösungen Ihnen dabei zur Verfügung stehen. So können Sie auf einen Blick die passende Strategie für unterschiedlichste Kundenumgebungen aufstellen und die Projektplanung proaktiv angehen.

Die wichtigsten Eckdaten der Datenschutz-Grundverordnung

- Gilt vollumfänglich seit dem 25. Mai 2018
- Betrifft den Umgang mit personenbezogenen Daten (pbD), also “[...] alle(n) Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; [...]”²
 - Beispiel: Name, Geburtsdatum, E-Mail- oder IP-Adresse
- Betrifft alle Unternehmen, die pbD erheben und verarbeiten³
- Gilt unabhängig vom Standort des Unternehmens oder der verarbeitenden Instanz⁴
- Bei Verstößen können Bußgelder in Höhe von bis zu 20 Millionen Euro oder 4% des weltweit erzielten Vorjahresumsatzes erhoben werden.⁵

2. Artikel 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung

Der Schutz Ihrer Kundensysteme vor Ransomware, Viren, Trojanern, Datendiebstahl und -manipulation ist eine der grundlegendsten Maßnahmen, wenn es um das Thema Datensicherheit und -schutz geht. Ein vielschichtiges Security-Konzept entspricht dabei auch der Forderung nach der “Sicherheit der Verarbeitung”, die Artikel 32⁶ aufstellt.

Eine vielschichtige Sicherheits-Architektur, welche Ihre Kunden gegen Datendiebstahl und -manipulation absichert, ist der erste Schritt zu einer möglichen technischen Umsetzung.

Welche Rahmenkriterien für ein solches Security-Konzept gelten und welche Grundsätze hier zum Tragen kommen, erfahren Sie nun im zweiten Teil unserer Serie: Hier beleuchten wir vor allem den Artikel 25 zum [“Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen”](#). Obwohl dieser Artikel sich auf alle technischen Prozesse abbilden lässt, spielen Security-Lösungen hier eine besonders wichtige Rolle: Als proaktive Maßnahme kommen sie von sich aus schon den Kernanforderungen nach, welche Artikel 25 an Datenschutzmaßnahmen stellt.

Als Grundlage definiert Artikel 25, dass der Verantwortliche – also dasjenige Unternehmen, welches in erster Instanz pbD seiner Kunden erhebt – “[...] geeignete technische und organisatorische Maßnahmen [...] (trifft), die darauf ausgelegt sind, Datenschutzgrundsätze wirksam umzusetzen”.⁷

Artikel 25 behandelt zwar die Anforderungen, denen die zum Datenschutz getroffenen Maßnahmen – und damit auch die eingesetzten Sicherheitstechnologien – folgen sollten, bestimmt dabei allerdings keine konkreten Kriterien. Vielmehr nennt der Artikel zwei einander ergänzende Konzepte, aus denen sich ein Rahmenkatalog ableiten lässt. Bei der Wahl der richtigen Lösung und der Einordnung der vorhandenen Strukturen kann dieser als Richtlinie herangezogen werden.

Privacy by Design

Art. 25 Abs. 1 behandelt vor allem die Machart der eingesetzten Lösungen: Bereits der zu Grunde liegende Aufbau sollte so gestaltet sein, dass sie den Datenschutz unterstützt. Dieser Anspruch spiegelt sich in dem Grundsatz “Privacy by Design” wider, aus dem sich einige Rahmenkriterien ableiten lassen.⁸ Diese können Sie unter anderem in der Beurteilung der DSGVO-Konformität einer Lösung unterstützen und Ihnen dabei helfen, Handlungspotenziale bei Ihren Kunden aufzudecken.

Privacy by Design

- Die Lösung sollte proaktiv arbeiten, bspw. vor Viren-Angriffen schützen.
- Der Datenschutz sollte in das Design integriert sein, bspw. über Zugriffskontrollen oder Verschlüsselung.
- Die Bedienung sollte transparent und nutzerzentriert gestaltet sein.
- Die Lösung sollte die Datenminimierung unterstützen.
- Die Sicherheit muss durchgehend gewährleistet sein, was sich in der Marktfähigkeit der Lösung widerspiegelt.

Privacy by Default

Ergänzend zur datenschutzfreundlichen Gestaltung, der die Lösung von sich aus schon folgt, formuliert Art. 25 Abs. 2 auch den Anspruch der “Privacy by Default”.⁹ Im Umgang mit personenbezogenen Daten stehen hier vor allem die Aktionsmöglichkeiten des Nutzers bei der Handhabung im Vordergrund sowie die Konfigurationsmöglichkeiten, welche die Lösung bietet:

Privacy by Default

- Die Lösung sollte sich so konfigurieren lassen, dass nur diejenigen Daten erhoben werden, welche zum Betrieb nötig sind.
- Die Konfiguration lässt sich auf die Menge der erhobenen pbD, den Umfang ihrer Verarbeitung, die Speicherfrist sowie die Zugänglichkeit anwenden.
- Werden keine weiteren Einstellungen getroffen, dürfen dadurch die pbD nicht anderen Personen zugänglich sein.

3. Maßnahmen zum Datenschutz: die technische Umsetzung

Ein erster Schritt zum Datenschutz ist die Sicherung des Unternehmensnetzwerks vor Ransomware, Viren oder Hackerangriffen.

Das Konzept “Datenschutz”, wie von der DSGVO gefordert, lässt sich nicht mit einer einzelnen Maßnahme abdecken. Vielmehr müssen personelle, organisatorische und technische Prozesse ineinandergreifen, wollen Ihre Kunden die Datenverarbeitung DSGVO-konform gestalten. Ein erster Schritt zum Datenschutz ist die Sicherung des Unternehmensnetzwerks vor Ransomware, Viren oder Hackerangriffen – denn diese haben die Unternehmensdaten Ihrer Kunden zum Ziel.

Neben Mitarbeitersensibilisierung und der klaren Definition von Prozessen im Umgang mit Daten ist damit ein mehrschichtiger Security-Ansatz ein unverzichtbarer Baustein. Der proaktive Ansatz, den Security-Lösungen verfolgen, kommt damit bereits von sich aus dem Konzept der “Privacy by Design” nach, das Artikel 25 als grundlegende Voraussetzung beim Datenschutz behandelt. Noch dazu sind solche Maßnahmen organisatorisch und unternehmerisch unverzichtbar, betrachtet man die unterschiedlichen Cyber-Bedrohungen, denen Ihre Kunden im Arbeitsalltag gegenüber stehen.

Sobald eine Verbindung zum Internet besteht, potenziert sich das Risiko für Ihre Kundensysteme – von Phishing über Exploit-Kits auf manipulierten Webseiten bis hin zu Ransomware. Selbst wenn die Internetnutzung außer zum Nachrichtenaustausch unterbunden ist, bleibt mit dem E-Mail-Verkehr das am häufigsten genutzte Einfallstor für Malware offen, wenn Spam-Nachrichten Mitarbeiter zu unvorsichtigen Klicks und Downloads verleiten.

Während ein Inselsystem ohne jedwede Art von digitaler Anbindung kaum praktikabel ist, ist es außerdem weiterhin angreifbar, denn: Infrastrukturen und Netzwerke können auch von innen heraus angegriffen werden. Nicht autorisierte Geräte mit Zugang zur Netzwerkinfrastruktur, unerlaubte Zugriffe auf kritische Unternehmensdaten und unbemerkte Datenflüsse nach außen – beispielsweise über Anwendungen auf Mitarbeiter-Geräten – sind nicht zu unterschätzende Gefahrenquellen.

Als IT-Profi stehen Sie dabei vor der Herausforderung, für Ihre Kunden die am besten geeignete Lösung zu finden, die sich gleichzeitig ideal in Ihr Service-Portfolio einfügt.

Um Ihnen die Übersicht und die Projektplanung zu erleichtern, haben wir die wichtigsten Rahmenkriterien aus Artikel 25 und anderen technisch anwendbaren Gesetzesabschnitten für Sie aufbereitet und mit Stichworten zur Zuordnung versehen:

“ [...] trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen, die darauf ausgelegt sind, die Datenschutzgrundsätze [...] wirksam umzusetzen [...]” (Art. 25 Abs. 1 DSGVO)

Privacy by Design

“Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.” (Art. 25 Abs. 2 DSGVO)

Privacy by Default

“Der Verantwortliche setzt geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.” (Art. 24 Abs. 1 DSGVO)¹⁰

Verantwortung des Verantwortlichen

Es müssen Maßnahmen getroffen werden, um die Vertraulichkeit und Integrität der Daten zu gewährleisten. (Art. 32 Abs. 1 lit. b)¹¹

Sicherheit der Verarbeitung



3.1 ESET – Sicherheit auf allen Ebenen

ESET, einer der weltweit führenden Hersteller von IT-Sicherheitslösungen, schützt Unternehmen jeglicher Größenordnung mit modernster Security-Software und bietet effizienten, leistungsfähigen Schutz vor Cyber-Bedrohungen jeder Art. Bereits seit Jahren am Markt etabliert und vielfach ausgezeichnet, überzeugt ESET mit wirkungsvoller und proaktiver Gefahrenerkennung, großer Benutzerfreundlichkeit sowie einem geringen Ressourcenverbrauch. Dabei können Sie zwischen dem ESET MSP-Programm und der On-Premises-Variante entscheiden.

Wie erfüllt ESET die DSGVO?

Privacy by Design

- ESET-Lösungen schützen proaktiv vor Cyber-Bedrohungen – die cloudbasierte ESET LiveGrid-Technologie bietet dabei schnellstmögliche Erkennung von Schädlingen.
- Konstante Weiterentwicklung der Software und durchgehend aktualisierte Datenbanken gewährleisten höchsten Netzwerkschutz.
- Verschiedene Features wie Exploit-Schutz, hocheffiziente Antiviren- und Anti-Spyware-Funktionen, sicheres Online-Banking, Botnet-Erkennung und eine Zwei-Wege-Firewall bieten ineinander greifend umfassende Netzwerksicherheit für jede Unternehmensgröße.

Privacy by Default

- Es werden so wenig Daten erhoben wie möglich.
- Es werden keine Endkundendaten verarbeitet.

Verantwortung des Verantwortlichen

- Protokollfunktionen sind über den ESET Remote Administrator abbildbar.

Sicherheit der Verarbeitung

- Über ESET Endpoint Encryption bieten Sie sichere Verschlüsselung von Festplatten, Wechselmedien, Dateien und E-Mails via FIPS 140-2-validierter 256-Bit-AES-Verschlüsselung.
- Mit ESET Secure Authentication sind Zugriffe unkompliziert und effizient durch ein zweites, einmalig generiertes Passwort geschützt, das via Smart Device oder Phone abgerufen werden kann.

4. IT-Security und Datenschutz: Was sind Ihre nächsten Schritte?

Ein mehrschichtiger IT-Security-Ansatz ist eine grundlegende Maßnahme, wenn es um den Datenschutz geht. Artikel 25 nennt Ihnen einige Rahmenkriterien, welche Ihnen die Beurteilung des Status Quo erleichtern und Ihnen als Leitlinien bei der Wahl der geeigneten Lösung dienen können.

Identifizieren Sie also schon jetzt Handlungspotenziale und stellen Sie dank unseres breit gefächerten Portfolios die ideale Sicherheitsstrategie für Ihre Kunden auf.

Selbstverständlich stehen wir Ihnen bei Fragen rund um unsere Security-Lösungen gern zur Verfügung – lassen Sie uns einfach wissen, wie wir Sie unterstützen können und kontaktieren Sie uns.

Quellenangaben

1. Art 25, DSGVO <https://dsgvo-gesetz.de/art-25-dsgvo/>
2. Art. 4, Abs. 1 DSGVO, <https://dsgvo-gesetz.de/art-4-dsgvo/>
3. Art. 1, Abs. 1 DSGVO, <https://dsgvo-gesetz.de/art-2-dsgvo/>
4. Art. 3 DSGVO, <https://dsgvo-gesetz.de/art-3-dsgvo/>
5. Art. 5 Abs. 3 DSGVO, <https://dsgvo-gesetz.de/art-83-dsgvo/>
6. <https://dsgvo-gesetz.de/art-32-dsgvo/>
7. Art. 25, Abs. 1 DSGVO, <https://dsgvo-gesetz.de/art-25-dsgvo/>
8. <https://dsgvo-gesetz.de/erwaegungsgruende/nr-78/>
9. <https://dsgvo-gesetz.de/erwaegungsgruende/nr-78/>
10. <https://dsgvo-gesetz.de/art-24-dsgvo/>
11. <https://dsgvo-gesetz.de/art-32-dsgvo/>

Rechtlicher Hinweis

Dieses Dokument dient lediglich der Information und stellt keine Rechtsberatung dar. Im konkreten Einzelfall wenden Sie sich bitte an einen spezialisierten Rechtsanwalt oder einen Datenschutzbeauftragten. Eine Gewähr und Haftung für die Richtigkeit aller Angaben wird nicht übernommen.

ELOVADE ▲

Kontakt Daten für Deutschland & Österreich:

ELOVADE Deutschland GmbH

sales@elovade.com

DE: +49 6441 67118 0

AT: +43 820 0010 36

elovade.com

Kontakt Daten für die Schweiz:

ELOVADE Swiss AG

sales@elovade.ch

CH: +41 55 552 27 00

elovade.ch