Leitfaden zur EU DS-GVO

Europäische Datenschutz-Grundverordnung

SECUREPOINT SECURITY SOLUTIONS

Europäische Datenschutz-Grundverordnung

Das Thema Datenschutz ist weit mehr als nur ein Randthema oder eine lästige Pflicht. Seit Mai 2018 sind die Herausforderungen und Aufgaben für alle Unternehmen gestiegen. Durch die EU DS-GVO hat das Thema Datenschutz eine neue Priorität erhalten.

Datenschutz erhält neue Priorität!

Seit dem 25. Mai 2018 gilt die neue europäische Datenschutz-Grundverordnung (EU DS-GVO) vollumfänglich. Mit diesem Leitfaden möchten wir Sie bei Ihrer Datenschutz-Aufgabe unterstützen.

Leitfaden zur Europäischen Datenschutz-Grundverordnung

Die Digitalisierung sorgt für bequemeres Einkaufen, schnelleres Navigieren, optimales Suchen oder einfach für eine persönliche Begrüßung von elektronischen Helfern. Die digitalen Dienstleister speichern und verarbeitet dafür Daten von (natürlichen) Personen, um all diese Prozesse zu Standards werden zu lassen. Dass Unternehmen verantwortungsbewusst mit diesen Daten umgehen, setzen Kunden in dieser digitalen Gesellschaft als selbstverständlich voraus.

Mit der „Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr" (kurz EU DS-GVO) hat die Europäische Union erstmals einheitliche Datenschutzregeln für einen der größten Wirtschaftsräume der Welt erlassen.

Die Verordnung hat das in Deutschland geltende Bundesdatenschutzgesetz (BDSG) weitgehend ersetzt und ist ein effizientes Werkzeug, um Personen und deren Daten nachhaltig zu schützen.

Das Thema Datenschutz ist somit weit mehr als nur ein Randthema oder lästige Pflicht. Seit dem 25. Mai 2018 sind die Herausforderungen und Aufgaben für alle Unternehmen gestiegen.

Die drohenden Strafen für die Nichteinhaltung der Vorschriften sind enorm hoch und der Handlungsbedarf entsprechend groß. Das gilt z. B. für den internen Umgang mit Mitarbeiterdaten, Prozessen, etc., aber besonders bei externen Daten, wie Kundendaten im Rahmen der Verarbeitung, Speicherung sowie Löschung.

Besonders im IT-Bereich haben sich eine Vielzahl von neuen Aufgaben und Maßnahmen ergeben, die im Systemhausgeschäft zu meistern sind. Mit diesem Leitfaden wollen wir helfen, die ersten wichtigen Informationen und Grundsätze der EU DS-GVO zu benennen.

Punkt 1
Was ist die EU Datenschutz-Grundverordnung (EU DS-GVO)?

Das europäische Parlament verabschiedete im April 2016 die Regelung der europaweiten Modernisierung und Vereinheitlichung von Datenschutzgesetzen durch die EU Datenschutz-Grundverordnung (EU DS-GVO).

Die EU DS-GVO baut auf mehreren Grundsätze auf und gibt entsprechende Prinzipien und unternehmerisches Handeln vor:

- Rechtmäßigkeit (Verbot mit Erlaubnisvorbehalt)
- Treu und Glauben (Verhältnismäßigkeit)
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Die Verordnung hebt die Richtlinie 95/46/EG von 1995 auf. Anders als die bisherige Richtlinie, ist die EU DS-GVO keine Richtlinie, sondern gilt wie ein Gesetz, das unmittelbar Strafen nach sich zieht.

Die Verordnung ist schon seit dem 24. Mai 2016 gültig und hatte eine Umsetzungsfrist von 2 Jahren, bis zum 25. Mai 2018. Bis zu diesem Termin hatten alle Unternehmen Zeit die Vorgaben der neuen EU DS-GVO umzusetzen.

Eine der wesentlichen Änderungen zu den vorherigen Regelungen ist, dass Unternehmen jederzeit geprüft werden können und die Einhaltung der Richtlinie nachweisen müssen. Damit drohen Sanktionen nicht erst bei Datenpannen, sondern können von den Aufsichtsbehörden schon im Vorfeld geahndet werden.

Die Aufsichtsbehörden sollen sicherstellen, dass die Geldbußen für Verstöße gegen die Verordnung „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sind".

Punkt 2
Welche Unternehmen sind von der EU DS-GVO betroffen?

Die EU DS-GVO regelt den Schutz und Umgang von personenbezogenen Daten, also deren Verarbeitung. Somit sind sämtliche öffentliche und nicht öffentliche Stellen betroffen, die personenbezogenen Daten verarbeiten.

Was sind eigentlich personenbezogene Daten?

„Im Sinne dieser Verordnung bezeichnet der Ausdruck 'personenbezogene Daten' alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;" Diese Erklärung ist sehr wortreich und weit gefasst.

Personenbezogene Daten sind demnach all jene Informationen, die sich auf eine natürliche Person beziehen, jedenfalls zumindest beziehbar sind und auf diese Weise Rückschlüsse auf deren Persönlichkeit zulassen.

Typische Daten, die gesammelt bzw. verarbeitet und von der EU DS-GVO geschützt werden, sind: Name, Anschrift, E-Mail-Adresse, IP-Adresse, etc. In der Geschäftswelt geht es zusätzlich oft um Kundendaten, die z. B. in einem ERP/CRM-System verarbeitet werden, d. h. Gesprächsnotizen, Geburtstage, Mailverläufe. Hinzu kommen weitere Daten, die z. B. nur für Marketingzwecke verwendet oder auch als „Zufallsprodukt" erfasst werden, wie IP-Adressen in einem Logfile, die von der EU DS-GVO geschützt sein können.

Punkt 3
Was passiert bei Verstößen?

Die Bußgelder für Unternehmen, die ihren Pflichten im Rahmen der EU DS-GVO nur mangelhaft oder gar nicht nachkommen, wurden neu festgelegt und sind dementsprechend empfindlich. Sollte eine Aufsichtsbehörde einen Verstoß feststellen, können Bußgelder bis zu 20 Million Euro oder von bis zu 4 % des weltweiten Firmenjahresumsatzes festgelegt werden.

Die Verhängung von Geldbußen soll laut EU DS-GVO in jedem Fall „wirksam, verhältnismäßig und abschreckend" sein. Neu ist auch, dass mit der EU DS-GVO Strafen gegen natürliche Personen vorgesehen sind und nicht nur gegen Unternehmen.

Damit kann auch ein Geschäftsführer persönlich oder unter Umständen auch der Datenschutzbeauftragte persönlich für Verstöße haftbar gemacht und ggf. in Regress genommen werden.

Punkt 4
Welche Rechte haben Kunden in der EU DS-GVO?

Die EU DS-GVO bestimmt die Spielregeln die Unternehmen einhalten müssen, wenn Sie personenbezogenen Daten verarbeiten. Einer der wichtigen Grundsätze dabei ist, dass die betroffene Person umfassend über ihre Rechte in klarer sowie verständlicher Sprache informiert werden muss und dass die Person ihre Rechte auf einfache Weise wahrnehmen kann.

Ein kurzer Überblick:

- **Einwilligung, Zweckbindung und Kopplungsverbot:**
Jede Person muss „umfassend und in einfacher Sprache" über den Verwendungszweck von Daten, die sie preisgibt, informiert werden. Die Einwilligung zur Nutzung muss freiwillig erfolgen – sie darf also nicht an andere Bedingungen geknüpft sein (z. B. das Einwilligen zur werblichen Zwecken der Daten, um eine Bestellung abschließen zu können etc.)

- **Auskunftsrecht:**
Verantwortliche eines Unternehmens müssen auf Verlangen der betroffenen Person kostenlos Auskunft über gespeicherte Daten, deren Verwendungszweck und ggf. Dritten die diese Daten erhalten haben, informieren.

- **Recht auf Vergessen werden – Löschpflicht:**
Der Kunde hat „das Recht zu verlangen, dass seine personenbezogenen Daten gelöscht werden". Die Löschpflichten und entsprechende Löschungsabsichten sind ein fester Bestandteil der EU DS-GVO. Es muss dazu bereits bei Aufnahme der Daten definiert werden, wann diese wieder gelöscht werden. Dabei dürfen die Daten nicht ohne Rechtsgrundlage länger als notwendig aufbewahrt werden.
Wurden die Daten an Dritte weitergegeben oder gar veröffentlicht, so muss der Verantwortliche auch sicherstellen, dass auch diese Daten gelöscht werden.

- **Umgehende Meldung an die Aufsichtsbehörde:**
„Im Fall einer Verletzung des Schutzes meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der Aufsichtsbehörde".

- **Recht auf Datenübertragbarkeit:**
Der Kunde hat das Recht, die über ihn gespeicherten Daten „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten". Einfach gesagt: Jedes Unternehmen muss jedem Kunden jederzeit seine personenbezogenen Daten in einem lesbaren Format aushändigen.

Punkt 5
Was ist jetzt wichtig?

In unserer Kompetenzreihe zum Securepoint EU DS-GVO Expert werden Sie in drei verschiedenen Schulungskursen tiefgreifende Informationen und Kenntnisse erlangen, u.a. zu oben angeführten und folgenden Punkten. Nur so sind Sie bestens gerüstet um für Ihre Kunden ein optimales Ergebnis sicher zu stellen. Bei Fragen zur Zertifizierung wenden Sie sich einfach an Ihren Ansprechpartner bei uns im Haus.

Obwohl die Übergangsfrist mittlerweile abgelaufen ist, haben viele Firmen nach wie vor kaum oder gar keine Vorkehrungen getroffen.

Das Marktforschungsinstitut Gartner hat ermittelt, dass bis Ende 2018 bei mehr als der Hälfte von der EU DS-GVO betroffenen Unternehmen nicht alle entsprechenden Vorgaben umgesetzt sind.

Laut einer Bitkom Studie aus 09/2017 ignorierte jedes dritte Unternehmen die EU DS-GVO und erst 13 Prozent aller befragten Unternehmen hatten überhaupt erste Maßnahmen eingeleitet.

Datenschutzbeauftragten benennen

Zunächst ist die Benennung oder Bestellung eines Datenschutzbeauftragten vorzunehmen, vor allem wenn bei dem Unternehmen besonders risikoreiche Datenverarbeitung erfolgt. Auch für kleine und mittelständische Firmen kann die Benennung eines externen Datenschutzbeauftragten eine gute Option sein.

Der Datenschutzbeauftragte muss ggf. gegenüber der Öffentlichkeit und auch der gegenüber der zuständigen Landesdatenschutzbehörde als offizieller Ansprechpartner benannt werden. Besonders im Fall einer Datenschutzverletzung ist es enorm wichtig einen zentralen Ansprechpartner zu haben, der alles Weitere organisiert, sich zügig, direkt und weitestgehend mit der Aufsichtsbehörde abstimmt, um noch größere Schäden zu vermeiden.

Erste Schritte zur Einführung der EU DS-GVO

Folgende Fragen können dabei helfen, die Gefahrenpunkte für die Umsetzung zu lokalisieren:

- Ist der Betroffene ausreichend und in einfacher Sprache informiert worden?
- Liegen ausreichend wirksame Einwilligungen der Betroffenen vor?
- Welche Daten werden im Unternehmen gesammelt oder verarbeitet?
- Werden die Daten ausreichend geschützt?
- Entspricht die eingesetzte IT dem aktuellen Stand der Technik?
- Kann eine Meldung an die Aufsichtsbehörde innerhalb von 72 Stunden durchgeführt werden?
- Können Kunden mit einfachen Mitteln eine Auskunft über ihre personenbezogenen Daten erhalten?
- Kann die Löschung der Daten durchgeführt werden?
- Werden Daten zur Speicherung oder Verarbeitung an Dritte übermittelt?
- Was und wie wird dokumentiert?

Verzeichnis von Verarbeitungstätigkeiten

Um überhaupt zu wissen, welche personenbezogenen Daten gespeichert und verarbeitet werden, ist eine Bestandsaufnahme unabdingbar. Die EU DS-GVO sieht das in dem „Verzeichnis von Verarbeitungstätigkeiten" vor. Auch wenn die Vorschrift Ausnahmen kennt, bei denen Unternehmen kein Verzeichnis führen müssen, empfehlen wir dringend, ein den Vorschriften entsprechendes Verzeichnis zu erstellen. Damit erhält der Verantwortliche einen Überblick und es wird gleichzeitig eine zentrale Anforderung der Vorschrift erfüllt.

Prozesse und Werkzeuge überprüfen

Es ist wichtig, sowohl die Mitarbeiter für den Datenschutz zu sensibilisieren, als auch Prozesse zu überprüfen. Die Erstellung von Richtlinien, die den Umgang mit personenbezogenen Daten festlegen, ist ein wichtiger Bestandteil. Diese Richtlinien stellen eine Ansammlung aus technischen sowie organisatorischen Maßnahmen dar.

IT-Infrastruktur überprüfen und absichern – „Privacy by Design" und „Privacy by Default"

Ein wichtiger Faktor ist die verantwortungsvolle Absicherung der IT-Systeme. Die vorhandene IT muss geprüft und ggf. durch neue ersetzt werden. Die EU DS-GVO führt die Begriffe „data protection by design" („Privacy by Design") und „data protection by default" („Privacy by Default") ein. Die Technik der Datenverarbeitung muss von vornherein auf diese Zwecksetzung ausgerichtet sein. Die Voreinstellungen müssen datenschutzkonform ausgewählt sein.

Die Absicherung fängt bereits auf der Netzwerk- und Kommunikationsebene an. Um ausschließlich vertrauenswürdige Verbindungen zu autorisieren, muss eine professionelle Firewall installiert werden. Bei der Auswahl der Firewall ist es empfohlen, darauf zu achten, dass der Hersteller seine Produkte gemäß der EU DS-GVO entwickelt sowie die Weitergabe von Daten an Dritte ausgeschlossen ist. Produkte, die Voraussetzungen von nicht EU-Staaten erfüllen, laufen Gefahr, gegen die Regelungen und Vorgaben der EU DS-GVO zu verstoßen. Achten Sie auf entsprechende Auszeichnungen oder Gütesiegel.

SecurITy made in Germany

NO BACKDOORS GARANTIE

In der Verordnung soll die Vorgabe des Datenschutzes durch Technik sowie einer datenschutzfreundlichen Voreinstellung erfüllt werden.

Auch die Datensicherung und der Schutz vor Datenverlust hat eine hohe Bedeutung. Um sicherzustellen, dass Daten nicht verloren gehen können, muss ein Backup/Restore und Recovery-Konzept erarbeitet werden. Hier kann zum Beispiel ein georedundantes Cloud-Backup in ein vertrauenswürdiges Rechenzentrum eine Lösung sein. Wichtig ist, dass Konzepte erstellt, dokumentiert und umgesetzt werden, um die Vorgaben der EU DS-GVO bestmöglich zu erfüllen.

Securepoint hilft Ihnen bei der Einhaltung der EU DS-GVO und Realisierung von Lösungskonzepten

Ob bei Ihnen im Unternehmen oder bei der Ausarbeitung von Konzepten zur Unterstützung Ihrer Kunden: Mit unseren Kompetenzreihen zum Thema EU DS-GVO können Sie sich wertvolles Know-how aufbauen und Ihren Kunden somit bestmögliche Unterstützung und Lösungen bieten.

Um die technischen Anforderungen der EU DS-GVO zu erfüllen, müssen die IT-Technik für die Infrastruktur und die Prozesse optimal aufeinander abgestimmt sein. Eine professionelle IT-Security Umgebung ist eine der tragenden Säulen: „Privacy by Design" und „Privacy by Default". Dazu gehören eine sorgfältige Dokumentation und eindeutige Abläufe bei einer Datenschutzverletzung. Das gilt sowohl für die schnelle Information und Reaktion des IT-Verantwortlichen sowie für eine umgehende Meldung an die Aufsichtsbehörden.

Securepoint bietet mit den „EU DS-GVO ready" ausgezeichneten Produkten und den Kompetenzen im Bereich „Managed Security" Komplett-Lösungen für Unternehmensnetzwerke jeder Größe.

Mehr Informationen zu den Securepoint Lösungen finden Sie unter www.securepoint.de

Bitte beachten Sie, dass dieser Leitfaden als Denkanstoß zu den möglichen Auswirkungen der EU DS-GVO gedacht ist und eine umfassende rechtliche Beratung nicht ersetzt.

Quellen:
https://www.gartner.com/newsroom/id/3701117
https://www.bitkom.org/Presse/Presseinformation/Jedes-dritte-Unternehmen-hat-sich-noch-nicht-mit-der-Datenschutzgrundverordnung-beschaeftigt.html
https://www.datenschutz-grundverordnung.eu/

Leitfaden zur Europäischen Datenschutz-Grundverordnung

IT-Security made in Germany

Securepoint ist Mitglied des deutschen IT-Sicherheitsverbands TeleTrusT. Die Securepoint-Lösungen für Netzwerksicherheit, Virenschutz, Sicherheit für mobile Geräte sowie E-Mail-Archivierung besitzen das Qualitätszeichen „IT-Security made in Germany". Securepoint erfüllt mit seinen Kompetenzen und seinen Produkten alle geforderten wichtigen Kriterien:

- Der Hauptsitz der Forschung und Entwicklung ist in Deutschland
- Die Gewähr vertrauenswürdiger Sicherheitslösungen
- Die Verpflichtung zu keinerlei versteckten Zugängen für Dritte (**keine Backdoors**)
- Die Zusicherung, dem deutschen Datenschutzrecht zu entsprechen

Partner und Kunden von Securepoint erhalten durch dieses Qualitätszeichen die Sicherheit, sich für IT-Security-Produkte zu entscheiden, die den strikten Richtlinien der EU DS-GVO unterliegen.

Erfüllen Sie mit der Securepoint UTM-Firewall technische Netzwerksicherheit

Alle Experten sind sich einig, das ohne die Verwendung einer UTM-Firewall die Einhaltung der Datenschutzbestimmungen nicht möglich ist.

- Schutz vor Datenverlust
- Absicherung von Kommunikation
- Zugriffsschutz und Zugriffsrechte durchsetzen
- Trennung verschiedener Abteilungen/Datenbestände

Erfüllen Sie mit der E-Mail Archivierung UMA die EU DS-GVO Anforderungen

E-Mail-Datenverkehr enthält oft sehr personenbezogene und somit schützenswerte Daten. Zum Datenschutz gehört unter anderem:

- Archivierung nach GoBD
- Nachweisliche unveränderliche Ablage (BSI TR-03125)
- Verschlüsselte Speicherung
- Schutz vor unbefugtem Zugriff
- Daten zuverlässig Wiederfinden
- Definiertes und protokolliertes Löschen

Änderungen und Irrtümer vorbehalten

SECUREPOINT SECURITY SOLUTIONS

Securepoint GmbH
Bleckeder Landstraße 28
21337 Lüneburg
Deutschland

Tel.: 0 41 31 / 24 01-0
Fax: 0 41 31 / 24 01-50
E-Mail: info@securepoint.de
Web: www.securepoint.de

EU DS-GVO ready

SecurITy made in Germany

Systemhaus/Partner: