TRUST IN GERMAN SICHERHEIT

G DATA Whitepaper

Die neue EU-Datenschutz-Grundverordnung – Was Unternehmen unbedingt wissen müssen

G DATA Software AG | September 2017

Einführung

Datenschutz ist mehr als eine Pflichtnummer: Die erneuerte EU-Datenschutz-Grundverordnung (DS-GVO) setzt das Thema jetzt europaweit auf die Agenda. Bis zum 25. Mai 2018 müssen Unternehmen sich an die neue Rechtslage anpassen und die Daten ihrer Kunden effektiv schützen. Die Strafen für das Nichteinhalten der neuen Verordnung sind empfindlich und der Handlungsbedarf ist entsprechend akut. Mitarbeiter müssen informiert und Workflows und Tools überprüft werden, um sicherzustellen, dass Kundendaten gesetzestreu verarbeitet werden. Auch im Bereich IT fällt hier eine beträchtliche Anzahl an Maßnahmen an. In diesem Whitepaper finden Sie die wichtigsten Anforderungen der Datenschutz-Grundverordnung und erfahren, wie eine ganzheitliche IT-Sicherheitslösung Sie bei der Einhaltung unterstützen kann.

1. Was ist die EU-Datenschutz-Grundverordnung?

Die EU-Datenschutz-Grundverordnung (DS-GVO) wurde im April 2016 vom europäischen Parlament verabschiedet und regelt die europaweite Modernisierung und Vereinheitlichung von Datenschutzgesetzen. Das Ziel ist das Garantieren des Schutzes von personenbezogenen Daten im Hinblick auf folgende Grundsätze[1]:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Die Verordnung ersetzt die in die Jahre gekommene Data Protection Directive (DPD) von 1995. Anders als die DPD ist die DS-GVO nicht „nur“ eine Richtlinie sondern tatsächlich ein Gesetz. Dies bedeutet, dass die Verordnung nicht separat von den EU-Mitgliedsstaaten implementiert werden muss. Das Datum des Inkrafttretens war deshalb schon der 24. Mai 2016. Um Unternehmen die Zeit zu geben, sich an die neue Gesetzeslage anzupassen, wurde eine Übergangsfrist bis zum 25. Mai 2018 eingeräumt. Bis zu diesem Datum haben Unternehmen Zeit, die Vorgaben der DS-GVO umzusetzen. Bleibt dies aus, können bei einer Datenschutzpanne hohe Bußgelder verhängt werden.

2. Welche Unternehmen sind von der DS-GVO betroffen?

Die Datenschutz-Grundverordnung regelt den Schutz von personenbezogenen Daten. Deshalb sind alle Unternehmen, die personenbezogene Daten von Privatpersonen in der europäischen Union verarbeiten, betroffen. Um deutlich zu machen, auf was für Daten das Gesetz sich bezieht, findet sich im Gesetzestext im Artikel 4 folgende Definition:

[1] Artikel 5 der DS-GVO. Den kompletten Gesetzestext finden Sie unter http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679.

> „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, identifiziert werden kann."

Die Definition ist also sehr weit gefasst. Typische Daten, die von Unternehmen gesammelt und von der DS-GVO geschützt werden, sind der Name, die Anschrift, die E-Mail-Adresse oder auch die IP-Adresse. Im Unternehmenskontext geht es dann oft um Kundendaten, die z. B. in einem CRM-System verarbeitet werden. Aber auch Daten, die nur für Marketingzwecke verwendet oder auch als „Beifang" aufgezeichnet werden, wie z. B. eine IP-Adresse in einer Log-Datei, werden von der DS-GVO geschützt.

3. Welche Rechte haben Kunden in der DS-GVO?

Die DS-GVO beschreibt die Vorgaben, die Unternehmen umsetzen müssen, wenn sie personenbezogene Daten verarbeiten. Obwohl viele Maßnahmen schon in der Data Protection Directive definiert wurden, gibt es ein paar neue Anordnungen, die selbst für Unternehmen, die bis jetzt immer „compliant" waren, eine Herausforderung darstellen werden. Ein kurzer Überblick:

- Recht auf Vergessenwerden: Kunden haben „das Recht zu verlangen, dass seine personenbezogenen Daten gelöscht werden" (Artikel 17).
- Zweckbindung und das Recht auf Zustimmung: Teilweise ist diese bereits im BDSG festgeschrieben, wird aber in der DS-GVO konkretisiert. Jeder Kunde muss „umfassend und in einfacher Sprache" über den Verwendungszweck von Daten, die er 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 Verwendung der Daten, um eine Bestellung abschließen zu können); dies ist im Erwägungsgrund Nr. 42 sowie 43 zur DS-GVO festgeschrieben.
- Zügige 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" (Artikel 33).
- Recht auf Datenübertragbarkeit: Kunden haben das Recht, die über sie gespeicherten Daten „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten" (Artikel 20).

Klar ist, dass die Umsetzung dieser Rechte und deren Abbildung in Unternehmensprozessen nicht trivial sind. Zum Beispiel setzen viele Vorgaben voraus, dass Unternehmen wissen, in welchem Umfang und an welchen Stellen sie personenbezogene Daten gespeichert haben. Das kann in einer kleinen Firma mit nur einer zentralen Kundendatenbank noch zutreffen, aber spätestens beim Betrachten von Datenquellen wie Videoüberwachungen in öffentlich zugänglichen Räumen oder auch bei Verarbeitung von Daten in Cloud-Plattformen (wie z. B. Salesforce) wird klar, dass viele

Firmen viel mehr personenbezogene Daten speichern und verarbeiten, als ihnen vielleicht bewusst ist und diese auch außerhalb des eigenen direkten Einflussbereichs gespeichert oder verarbeitet werden. Auch gibt es Konfliktpotenzial, wenn ein Kunde Daten löschen lassen möchte, diese aber im Rahmen von anderen Gesetzen aufbewahrt werden müssen (wie z. B. Rechnungsdaten).

4. Was passiert bei Verstößen gegen die DS-GVO?

Nicht nur die in der DS-GVO beschriebenen Maßnahmen sind neu: Auch die Bußgelder für Unternehmen, die diese entweder nicht oder nur mangelhaft umsetzen, wurden neu definiert. Wenn eine Datenschutzbehörde einen Verstoß feststellt, können – je nach Schwere eines Falls – folgende Bußgeldbeträge fällig werden:

- Bis zu € 20 Million Euro oder 4 % des weltweiten Firmenjahresumsatzes (der jeweils höhere Betrag wird angesetzt)
- Bis zu € 10 Million Euro oder 2 % des weltweiten Firmenjahresumsatzes (der jeweils höhere Betrag wird angesetzt)

Die erste Bußgeldkategorie wird zum Beispiel angewendet, wenn ein Unternehmen gegen Bestimmungen im Artikel 17 (Recht auf Vergessenwerden) verstößt. Letztere Kategorie ist für verhältnismäßig kleine Verstoße gedacht, wie z. B. eine Verletzung der Meldepflicht nach Artikel 33, kann jedoch bei einem Maximalbetrag von € 10 Million Euro oder 2 % des Umsatzes immer noch sehr hoch ausfallen. Die Bußgelder werden im Artikel 83 der DS-GVO definiert, der des Weiteren sicherstellt, dass die Verhängung von Geldbußen in jedem Fall „wirksam, verhältnismäßig und abschreckend“ ist. Für Deutschland hat sich seit dem Inkrafttreten der DS-GVO auch die Haftung geändert: Im Artikel 41 bis 43 des Datenschutz-Anpassungs- und -Umsetzungsgesetzes (DSAnpUG) sind auch Sanktionsmöglichkeiten gegen natürliche Personen vorgesehen, nicht nur gegen Unternehmen. Sprich: Auch ein Datenschutzbeauftragter oder ein Geschäftsführer kann für Verstöße persönlich haftbar gemacht und ggf. in Regress genommen werden.

5. Der Countdown läuft: Worauf kommt es an?

Trotz möglicher hoher Geldstrafen und der schnell ablaufenden Übergangsfrist haben viele Firmen noch keine Vorkehrungen getroffen. Laut Gartner wird bis Ende 2018, wenn die Verordnung schon längst in Kraft getreten ist, immer noch mehr als die Hälfte der von der DS-GVO betroffenen Unternehmen nicht alle Vorgaben umgesetzt haben[2]. Mit so vielen möglichen Auswirkungen ist es wichtig, einen Überblick über die Implementierungsschwerpunkte zu bekommen.

5.1. Datenschutzbeauftragten benennen

Der erste Schritt ist die Benennung oder Bestellung eines Datenschutzbeauftragten. Dies gilt gemäß Artikel 37 für Behörden, öffentliche Stellen und Unternehmen, die personenbezogene Daten verarbeiten; der Paragraph 4f des Bundesdatenschutzgesetzes (BDSG) geht hier noch weiter ins Detail. Für kleine und mittelständische Firmen kann auch die Benennung eines externen

[2] Quelle: https://www.gartner.com/newsroom/id/3701117.

Datenschutzbeauftragten in Betracht gezogen werden. Der Datenschutzbeauftragte muss sowohl gegenüber Öffentlichkeit wie auch der zuständigen Landesdatenschutzbehörde als offizieller Ansprechpartner benannt werden. Aber auch Firmen, die nicht zur Benennung eines Datenschutzbeauftragten verpflichtet sind, können davon profitieren, z. B. um eine Anlaufstelle für interne und externe Fragen bezüglich Datenschutz zu etablieren.

5.2. Brennpunkte identifizieren

Für jede Firma, egal welcher Größe, können folgende Fragen dabei helfen, die Brennpunkte für die Umsetzung zu identifizieren:

- Welche von der DS-GVO betroffenen Daten werden im Unternehmen gesammelt oder verarbeitet?
- Werden die Daten ausreichend geschützt? Entspricht die eingesetzte Technologie dem Stand der Technik?
- Kann im Fall einer Datenschutzverletzung eine Meldung an die Datenschutzbehörde innerhalb 72 Stunden verschickt werden?
- Können Kunden Auskunft über die über sie gespeicherten Daten bekommen bzw. kann die Löschung der Daten durchgeführt werden?
- Werden Daten zur Speicherung oder Verarbeitung an andere Unternehmen übermittelt (z. B. Cloud-Dienste)? Müssen hier gegebenenfalls Anpassungen in den Verträgen zur Auftrags-Datenverarbeitung vorgenommen werden? Wichtig hier: es gibt keinen „Bestandsschutz“ für Altverträge.

5.3. Workflows und Tools überprüfen

Dabei gilt es, sowohl die Mitarbeiter für das Thema zu sensibilisieren als auch die Workflows und Tools zu überprüfen und ggf. auf einen gesetzeskonformen Stand zu bringen. Die Erstellung von Compliance-Regeln, die den Umgang mit Informationen festlegen, ist hier ein wichtiger Schritt. Solche Regeln stellen eine Kombination aus technischen und organisatorischen Maßnahmen dar. So kann z. B. auf der Technologieebene ein Policy Management dafür sorgen, dass nur die für die Datenverarbeitung notwendigen Tools verwendet werden können – und Anwendungen wie z. B. private Cloud-Speicherdienste nicht. Auch die Benutzung von externen Geräten soll unterbunden werden, damit Mitarbeiter die personenbezogenen Daten nicht auf z. B. USB-Sticks abspeichern können.

5.4. IT-Infrastruktur überprüfen und absichern

Ein weiterer wichtiger Baustein ist die umfassende Absicherung der IT-Systeme. Bestehende Systeme müssen überprüft und neue Systeme ggf. eingeplant und ausgerollt werden. Der Schutz fängt schon auf der Netzwerk- und Kommunikationsebene an. Um unerlaubte Verbindungen zu unterbinden, soll eine Firewall verwendet werden. Web-Verkehr und andere Kommunikationswege aus dem Internet sollten gründlich überprüft werden, z. B. von einer Web-Schutz-Komponente oder auch einem E-Mail-Scan. Schutz gegen bösartige Malware kann mit Hilfe einer proaktiven Dateisystem- und Prozessüberwachung sichergestellt werden. Um dafür zu sorgen, dass das

Betriebssystem und die Anwendungen auf dem aktuellsten Stand sind und Schwachstellen rechtzeitig behoben werden, kann ein Patch-Management-System dabei helfen, den Überblick über die Patchverteilung zu behalten. Nicht zuletzt ist die Datensicherung sehr relevant: Um dafür zu sorgen, dass Daten nicht verloren gehen können, muss ein Backup- und Wiederherstellungskonzept erarbeitet werden.

G DATA unterstützt Sie bei der Einhaltung der DS-GVO

Um die technischen Anforderungen der DS-GVO erfüllen zu können, müssen die Schutzkomponente für die IT-Infrastruktur und Prozesse optimal aufeinander abgestimmt sein. Ein einheitliches Konzept für die Überwachung der Netzwerkinfrastruktur und die Benachrichtigung des Administrators im Fall eines möglichen Datenschutzvorfalles ist essenziell. G DATA bietet mit dem Layered Security-Ansatz eine komplette Lösung für Unternehmensnetzwerke jeder Größe, die einen ausgefeilten proaktiven Schutz mit effizienten und akkuraten Möglichkeiten für ein regelmäßiges Reporting und Vorfallbenachrichtigung kombiniert. Sie können die Business-Lösungen von G DATA auf eigener Hardware installieren und selber verwalten oder auch, falls gewünscht, mit Hilfe der SaaS-Lösung G DATA Managed Endpoint Security den Installations- und Verwaltungsaufwand auslagern. Herstellerunabhängige Beratungsleistungen wie z. B. Penetration-Tests werden von der G DATA Advanced Analytics GmbH angeboten.

Mehr Informationen zu den G DATA Business-Lösungen finden Sie unter www.gdata.de/business. Der G DATA Security Blog informiert Sie unter blog.gdata.de über die aktuellsten Entwicklungen in den Bereichen Datenschutz, Compliance und IT-Sicherheit. Mehr Informationen über die Beratungsleistungen der G DATA Advanced Analytics GmbH finden Sie unter www.gdata-advancedanalytics.de.

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