White Paper

DATENSCHUTZ-GRUNDVERORDNUNG

FÜR IT-ADMINISTRATOREN, ENTSCHEIDER UND INHABER MITTELSTÄNDISCHER UNTERNEHMEN

Compliance für KMU im Hinblick auf Datenspeicherung

Was ist die DSGVO?

Mit der **europäischen Datenschutz-Grundverordnung (DSGVO)** soll der Datenschutz für alle Personen innerhalb der Europäischen Union gestärkt und vereinheitlicht werden.

Darüber hinaus regelt die DSGVO auch den Export personenbezogener Daten in Länder außerhalb der EU. Unternehmen, die außerhalb der Europäischen Union ansässig sind, aber Daten über EU-Bürger speichern, unterliegen der DSGVO.

Ihr Hauptziel ist es, den Bürgern und Einwohnern die Kontrolle über ihre personenbezogenen Daten zurückzugeben und das Regelungsumfeld für internationale Unternehmen zu vereinfachen, indem die Regulierung innerhalb der EU vereinheitlicht wird.

Die DSGVO enthält hauptsächlich Informationen darüber, wie personenbezogene Daten verarbeitet werden sollen, und definiert die Rolle des Auftragsverarbeiters und des Verantwortlichen. Zudem enthält sie Angaben dazu, wie die Datenschutzprinzipien „Privacy by Design“ und „Privacy by Default“ angewandt werden sollen.

Die DSGVO tritt am 25. Mai 2018 in Kraft.

Auswirkungen der DSGVO

Kleine und mittlere Unternehmen (KMU), die über Daten von EU-Bürgern verfügen, sind für den Schutz der von ihnen gespeicherten Daten verantwortlich.

Diese Daten müssen systematisch gespeichert und vor Diebstahl und Missbrauch geschützt werden.

KMU müssen auch in der Lage sein, die in der DSGVO definierten Rechte der betroffenen Person einzuhalten, die wie folgt lauten:

- **Recht, über die Datenverarbeitung informiert zu werden**
- **Recht, auf die eigenen Daten zuzugreifen**
- **Recht, die eigenen Daten zu korrigieren oder zu löschen**
- **Recht, die eigenen Daten an ein anderes Unternehmen zu übertragen**

Auch die Datenaufbewahrung ist ein wichtiger Faktor. Einige Arten von Daten müssen nach Ablauf einer bestimmten Frist gelöscht werden, z. B. personenbezogene Daten, die im Zusammenhang mit einem Produktkauf und der damit verbundenen Gewährleistung erfasst werden.

Zudem gibt es andere Arten von Daten, die für einen bestimmten Mindestzeitraum aufbewahrt werden müssen, wie etwa bestimmte Finanzdaten.

In der Praxis bedeutet dies, dass KMU den Speicherort personenbezogener Daten kennen und in der Lage sein müssen, zeitnah auf Datenanfragen zu reagieren.

Unternehmen, die sich nicht an die Vorschriften der DSGVO halten, gehen im Fall einer größeren Systemverletzung enorme Risiken ein, etwa bei einem Hackerangriff mit Datendiebstahl aus einer Kundendatenbank.

Geldstrafen können sich auf bis zu 20 Millionen Euro oder vier Prozent des Jahresumsatzes belaufen, je nachdem, welcher Wert höher ist.

Notwendigkeit der Einhaltung der DSGVO

Die meisten großen Unternehmen tun ihr Möglichstes, um die Anforderungen der DSGVO zu erfüllen. Sie sind sich der Konsequenzen einer Datenschutzverletzung bewusst.

Kleine und mittlere Unternehmen legen jedoch eine eher abwartende Haltung an den Tag.

Sie sind der Meinung, dass die DSGVO hauptsächlich für große Unternehmen gilt, die riesige Mengen personenbezogener Daten sammeln und verarbeiten, wie z. B. soziale Netzwerke, Cloud-Provider oder Suchmaschinen.

Viele dieser Unternehmen warten ab, was passiert, wenn ein vergleichbares Unternehmen gegen die Gesetzgebung verstößt.

Dieser Ansatz ist äußerst riskant, da bei DSGVO-Strafen das Risiko der Zahlungsunfähigkeit oder gar Schließung des Unternehmens besteht.

Die DSGVO gilt für alle Unternehmen unabhängig von Größe oder Umsatz.

Datenschutzprinzipien „Privacy by Design“ und „Privacy by Default“

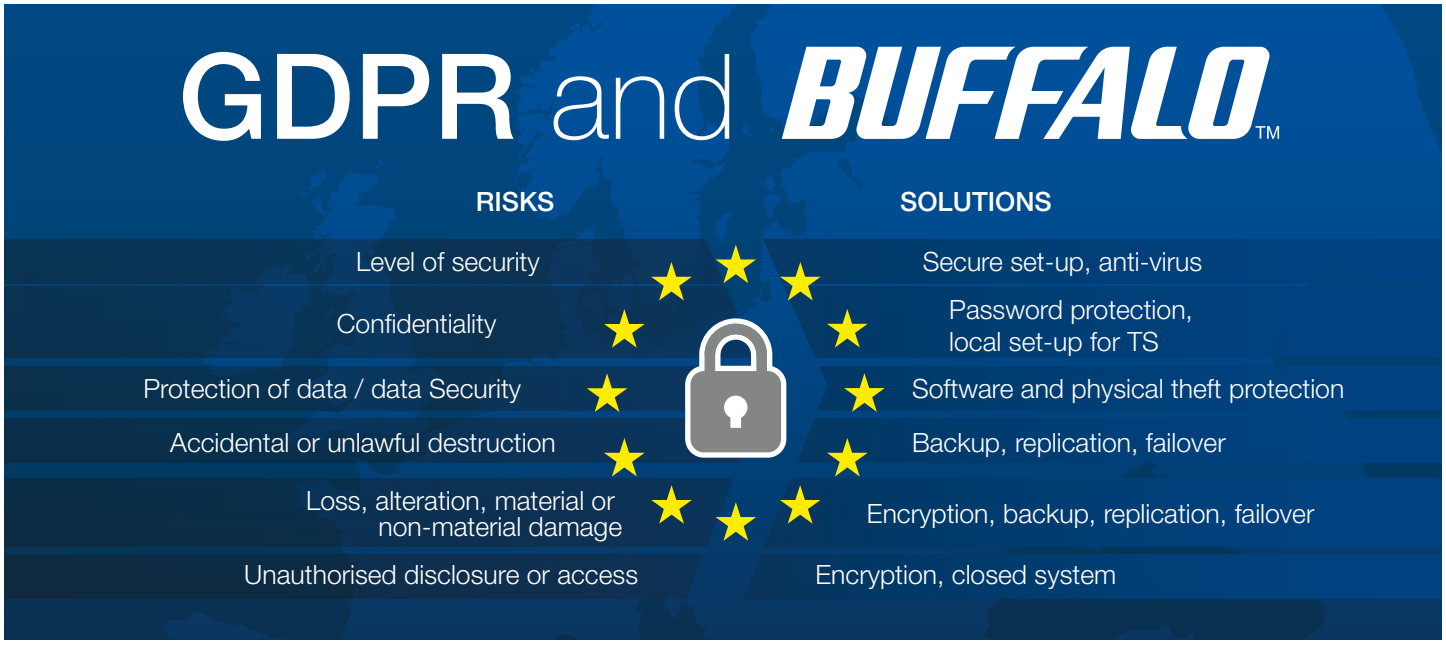
Im Rahmen des DSGVO-Mandats müssen Unternehmen sicherstellen, dass sie die Datenschutzprinzipien „Privacy by Design“ und „Privacy by Default“ umsetzen.

Vereinfacht gesagt bedeutet dies, dass Unternehmen ihre Systeme und Prozesse schützen müssen, um sicherzustellen, dass keine Datenlecks entstehen oder Hacker leichtes Spiel haben.

Dafür muss der Datenschutz bereits bei der Entwicklung, also dem Design, von Unternehmensprozessen für Produkte und Services integriert werden.

Dies setzt voraus, dass Datenschutzeinstellungen standardmäßig bereits zu einem frühen Zeitpunkt im Prozess festgelegt werden und technische und prozessbasierte Maßnahmen während des gesamten Lebenszyklus der Datenverarbeitung den Vorschriften entsprechen.

Darüber hinaus müssen Unternehmen Mechanismen implementieren, die sicherstellen, dass personenbezogene Daten nur verarbeitet werden, wenn dies für den jeweiligen Zweck erforderlich ist.



DSGVO-Datenschutz in der Praxis

Die Datenschutzprinzipien „Privacy by Design“ und „Privacy by Default“ wirken sich möglicherweise direkt auf Ihre Datenspeicherungslösung aus.

Die Anforderungen bedeuten, dass Sie eine Datenspeicherung benötigen, die sowohl leicht zugänglich und verwaltbar ist als auch grundlegende Datenschutz- und Sicherungsvorkehrungen aufweist.

- Wenn Sie vorhaben, Daten intern zu speichern, ist Ihr Unternehmen sowohl der Datenverantwortliche als auch der Datenverarbeiter. Aus diesem Grund haftet Ihr Unternehmen in vollem Umfang für die Folgen, falls diese Daten gehackt werden oder ein Verstoß gegen die Vorschriften vorliegt.

- Wenn Sie vorhaben, eine öffentliche Cloud- oder Hybrid-Speicherlösung zu verwenden, ist Ihr Unternehmen dafür verantwortlich sicherzustellen, dass es selbst und der Drittanbieter die DSGVO einhalten.

Wenn personenbezogene Daten intern auf einem Server, NAS (Network Attached Storage) oder anderen Geräten gespeichert werden, sollte das Speichergerät für die DSGVO-Compliance folgende Merkmale aufweisen:

- **Passwortschutz:** Geräte und Dateien bzw. Ordner, die personenbezogene Daten enthalten, sollten durch Passwörter geschützt werden. Sie sollten nur Benutzern zugänglich sein, die dazu berechtigt sind, auf die Daten zuzugreifen bzw. sie zu verarbeiten.

- **Verschlüsselung:** Daten sollten bei der Speicherung oder Übertragung immer verschlüsselt sein.

- **Physischer Schutz vor Diebstahl/Verlust:** Geräte, auf den personenbezogene Daten gespeichert sind, sollten physisch gesichert sein, z. B. durch ein Kensington-Schloss, abschließbare NAS und Festplatten in einem Server oder ähnliches.

- **Antivirensoftware,** die sicherstellt, dass Daten nicht mit Malware wie etwa Ransomware infiziert werden.

- **Firewall-Schutz**

- **Backup und Wiederherstellung:** Backups sollten automatisiert und täglich durchgeführt werden, damit im Fall eines Datenverlusts der aktuellste Stand der personenbezogenen Daten abgerufen werden kann.

Darüber hinaus gibt es eine Reihe weiterer zusätzlicher Maßnahmen, die ebenso wichtig sind:

- Ein Speichergerät, das RAID-Redundanz bietet und vor Festplattenausfällen schützt, verhindert Systemausfallzeiten und Datenverluste.

- Die zentrale Speicherung ist der lokalen Speicherung auf PCs, Laptops oder externen bzw. tragbaren Festplatten vorzuziehen. Diese Geräte sind anfälliger für Diebstahl und unbefugten Zugriff. Außerdem lässt sich nur sehr schwer kontrollieren, wer Zugang zu den Geräten und den darauf befindlichen Daten hat.

Geschlossenes System

Sichere Einrichtung

Daten-Verschlüsselung

Kennwörter

Anti-Virus
(TS3000/3010 & TS5000/5010, separat erhältlich)

Backup, Replikation, Failover und Verschlüsselung

Anti-Diebstahl-Funktionen
- Softwareschutz: Boot-Authentifizierung
- Physischer Diebstahlschutz

DSGVO-Grundlagen für KMU

Es gibt einige grundlegende Maßnahmen zur Speichersicherheit, die KMU ergreifen müssen, um sicherzustellen, dass sie die DSGVO-Mandate zum Schutz personenbezogener Daten erfüllen.

Root-Verzeichnis des Speichergeräts

Das Root-Verzeichnis ist wie der Stamm eines Baums, aus dem alle anderen Zweige hervorgehen. Wenn sich ein Hacker Zugriff auf ein Root-Verzeichnis verschafft, kann er Viren und Malware vor aller Augen verstecken, indem er böswilligen Code als wichtige Dateien tarnt, die von Antivirensoftware übersehen werden.

Aus diesem Grund müssen NAS-Betriebssysteme geschlossene Systeme sein, auf die selbst der Systemadministrator nicht zugreifen kann. Dadurch werden Schlupflöcher für Hacker geschlossen, die meist hochentwickelte Rootkit-Tools für den Zugriff auf Root-Verzeichnisse verwenden.

Sichere Einrichtung

Bei der Konfiguration von NAS-Systemen in Unternehmen ist oftmals eine Internetverbindung erforderlich, um das Konto einzurichten und den Fernzugriff zu ermöglichen. Bei einigen NAS-Systemen ist dies das Standardverfahren.

Es ist aber auch ein Verfahren, das Hacker zum Diebstahl von Benutzernamen und Passwörtern nutzen, wenn Daten außerhalb des Unternehmensnetzwerks über das Internet übertragen werden.

Starke Verschlüsselung

Auf Festplatten gespeicherte Daten können gestohlen werden. Wird die Festplatte mit der theoretisch nicht knackbaren 256 AES-Verschlüsselung verschlüsselt, können die Daten nicht gelesen werden, selbst wenn die Festplatte entfernt wird.

Buffalo TeraStation™– die sicherste NAS-Lösung mit kompletter DSGVO-Compliance

Das speziell für KMU entwickelte Buffalo TeraStation™ NAS bietet die folgenden Funktionen, die die vollständige DSGVO-Compliance sicherstellen.

- Es gibt keinen Zugang „durch die Hintertür“, das heißt, Hacker können nicht über gängige Methoden wie SSH-Protokolle oder Telnet-Server auf den Datenspeicher zugreifen. Kurz gesagt: Die Daten können weder gehackt noch zerstört werden.

- Die Betriebssystem-Firmware der TeraStation™ enthält keine Funktionen oder Optionen zum Ändern oder Hinzufügen von Merkmalen. Die Firmware ist im Grunde also gesperrt, so dass es keine Möglichkeit gibt, versehentlich Sicherheitslücken zu schaffen, die von Hackern ausgenutzt werden könnten.

- Über eine Softwareoption kann der Benutzer der Datensicherheit Priorität gegenüber dem Systemzugriff geben, indem externe Wiederherstellungen oder Rücksetzungen deaktiviert werden.

- Die physische Sicherung erfolgt bei der TeraStation™ durch Kabelschlösser und abschließbare Festplatten. Diese physischen Sicherungsmaßnahmen schützen die Hardware vor Diebstahl, während die Boot-Authentisierung in der Software den Datenzugriff unter allen Umständen verweigert.

- AES-Hardwareverschlüsselung für Festplattenlaufwerke ist verfügbar. Diese Funktion ist zwar nicht standardmäßig eingeschaltet, lässt sich aber leicht aktivieren. Die Festplatte wird damit im Prinzip gesperrt, sodass kein Datenzugriff möglich ist, falls die Festplatte entfernt wird.

- Bietet sichere Datenaustauschprotokolle (HTTPS, SFTP) für sicheren lokalen und Remote-Zugriff. Daten werden niemals unverschlüsselt über das Internet versendet, so dass sie nicht von Dritten oder Hackern gelesen werden können.

- Um die Leistung, Zuverlässigkeit und Sicherheit der Datenspeicherung zu verbessern, sind sichere RAID-Modi werkseitig vorkonfiguriert.

- Jede TeraStation™ bietet die Hot Swap-Funktion für den 24-Stunden-Festplattenaustausch, um sicherzustellen, dass der Speicher immer intakt ist.

- Die TeraStation™-Firmware kann nicht mit Viren infiziert werden, da es sich um ein geschlossenes System handelt. Dennoch besteht natürlich immer das Risiko, dass Dateien und freigegebene Dateien, die zwischen Computern, Tablets und Smartphones übertragen werden, mit Malware wie Ransomware, Spyware oder Trojanern infiziert sind, wenn diese Geräte mit dem Datenspeicher verbunden werden. Die Antiviren-Option, die regelmäßig mit den neuesten Virensignaturen aktualisiert wird und darauf ausgelegt ist, Zero-Day-Bedrohungen zu erkennen, hält alle Dateien frei von Malware.

- Es stehen mehrere Backup-Optionen zur Verfügung, um Dateien sicher auf dem NAS oder außerhalb davon zu speichern. Zu diesen Optionen gehören regelmäßige Backups, Datenreplikation, Failover, Cloud-Backup, USB- oder NAS-Backup und PC- und Server-Backup.

Es stehen mehrere Buffalo TeraStation™ Modelle zur Verfügung, von denen jedes speziell auf die Bedürfnisse von Unternehmen einer bestimmten Größe zugeschnitten ist.

Der Datenschutzbeauftragte

Von zentraler Bedeutung für die erfolgreiche DSGVO-Compliance bei KMU ist ein Datenschutzbeauftragter, der die Verantwortung für die Verwaltung und den Schutz von Kundendaten trägt.

Die Ernennung einer Einzelperson zum Compliance-Beauftragten stellt eine konsequente Fokussierung sicher.

Der Beauftragte kann Compliance-Lücken identifizieren, notwendige Schritte planen sowie Managementprozesse einführen und überwachen, die auf die Anforderungen abgestimmt sind.

Der Compliance-Beauftragte ist der Experte für DSGVO-Compliance im Unternehmen und damit der Dreh- und Angelpunkt für die erfolgreiche Einhaltung der Vorschriften.

DSGVO-Definitionen

In der DSGVO wird von Verantwortlichen, Auftragsverarbeitern und betroffenen Personen gesprochen.

- Verantwortliche sind Unternehmen, die Daten von EU-Bürgern erfassen, wie etwa ein Online- oder Offline-Unternehmen, das in der EU Handel betreibt und personenbezogene Kundendaten wie Namen, Adressen und Zahlungsdaten speichert.

- Auftragsverarbeiter sind Unternehmen, die Daten im Namen von Verantwortlichen verarbeiten, wie etwa ein Cloud-Service-Provider.

- Eine betroffene Person ist ein EU-Bürger oder eine in der EU ansässige Person, deren Daten von einem Verantwortlichen gespeichert oder von einem Auftragsverarbeiter verarbeitet werden.

Viele KMU sind wahrscheinlich zugleich Verantwortliche und Auftragsverarbeiter.

DSGVO-Definition personenbezogener Daten

Gemäß der DSGVO sind personenbezogene Daten alle Informationen über einen EU-Bürger, die zur direkten oder indirekten Identifizierung der Person verwendet werden können.

Dabei kann es sich um einen Namen, ein Foto, eine E-Mail-Adresse, eine Bankverbindung, Posts auf Social Networking-Websites, medizinische Angaben und sogar eine Computer-IP-Adresse handeln.