Risiko Datenpannen

So beugen Sie DSGVO-konform vor

Einleitung

Der Berufsalltag hat sich stark gewandelt und mit ihm althergebrachte Arbeitsweisen: Dank mobiler Speichermedien haben wir praktisch jederzeit von jedem Ort Zugriff auf unsere Daten und können überall arbeiten. Wir profitieren von der **permanenten Verfügbarkeit** geschäftlicher Informationen, können **mobile Arbeitsversionen** oder Sicherheitskopien anlegen und so unsere eigenen Arbeitszeiten optimieren und letztlich Vorgänge effektiv verkürzen.

Doch die Datenmobilität hat auch ihre Schattenseiten: Verlorene oder gestohlene USB-Sticks stellen ein ernstzunehmendes Risiko dar. Bereits **72 %** aller Unternehmen gaben in einer Studie* an, einzelne USB-Sticks nicht mehr finden zu können. Das ist besonders dramatisch, weil 25 % der befragten Unternehmen **sensible Daten** darauf gespeichert hatten. Solche Datenpannen untergraben das **Vertrauen der Kunden** in das betroffene Unternehmen und gehen daher immer mit einem Imageverlust und auch Kosten einher. Gefahren, die sich aufgrund von Veröffentlichung oder krimineller Nutzung der Daten daraus ergeben, sind dabei noch nicht eingerechnet.

Der Gesetzgeber hat auf die zunehmenden Gefahren von Datenpannen reagiert. Die **EU-Datenschutzgrundverordnung** (EU-DSGVO) nimmt ab Mai 2018 Unternehmen in noch größerem Maße in die Pflicht. Unter anderem droht sie mit empfindlichen Strafen bei Nichteinhaltung der vorgeschriebenen Maßnahmen.

In diesem Whitepaper erfahren Sie:

- Was Sie über Datenmobilität und Datenpannen wissen sollten
- Was die EU-DSGVO fordert und wie Unternehmen auf die neuen Regelungen reagieren müssen
- Was Sie konkret tun können, um Datenpannen zu vermeiden

Inhaltsverzeichnis

* Studie von Kingston Technology in Deutschland 2016 durchgeführt (Anzahl der Antworten: 200)

Die DSGVO setzt auf Prävention

Die europäische Datenschutzgrundverordnung (EU-DSGVO) ersetzt die bisherigen nationalen Regelungen zum Datenschutz und tritt nach einer 2-jährigen Übergangszeit am 25. Mai 2018 in Kraft. Oberstes Ziel der EU-DSGVO ist es, den **Daten- und Grundrechtsschutz für EU-Bürger** zu verbessern.

Die DSGVO gilt nicht nur für europäische Unternehmen, sondern für alle Organisationen, die EU-Bürgern (auch kostenfreie) Waren- und Dienstleistungen anbieten und dabei deren personenbezogene Daten erfassen. Zwischen Großkonzernen, Mittelstand oder kleinen Startups unterscheidet die DSGVO dabei nicht. Daher sollte der Datenschutz in allen Unternehmen, die personenbezogene Daten erheben, verarbeiten und speichern, überprüft werden.

Das Ziel, personenbezogene Daten zu schützen, wird mit empfindlichen Strafen verteidigt: Verletzungen des Datenschutzes, gegen die keine entsprechenden Maßnahmen getroffen wurden, können mit bis zu **4 % des konzernweiten Jahresumsatzes oder bis zu 20 Millionen Euro** geahndet werden.

Hinzu kommt, dass alle Datenschutzverletzungen sowohl der jeweils zuständigen Aufsichtsbehörde als auch den betroffenen Personen angezeigt werden müssen. Abgesehen von den Strafzahlungen können die Folgen für ein Unternehmen in Ansehen, Kundenvertrauen und Umsatz so sehr weitreichend sein.

Diese Maßnahmen sollen dafür sorgen, dass Datenpannen möglichst vermieden werden. Das Öffentlich-Werden von personenbezogenen Daten soll damit minimiert und Unternehmen zu vorbeugendem Verhalten angehalten werden. Der EU ist allerdings bewusst, dass absoluter Datenschutz nicht umsetzbar ist. Mit der neuen Verordnung soll dennoch die **bestmögliche Prävention** erzielt werden.

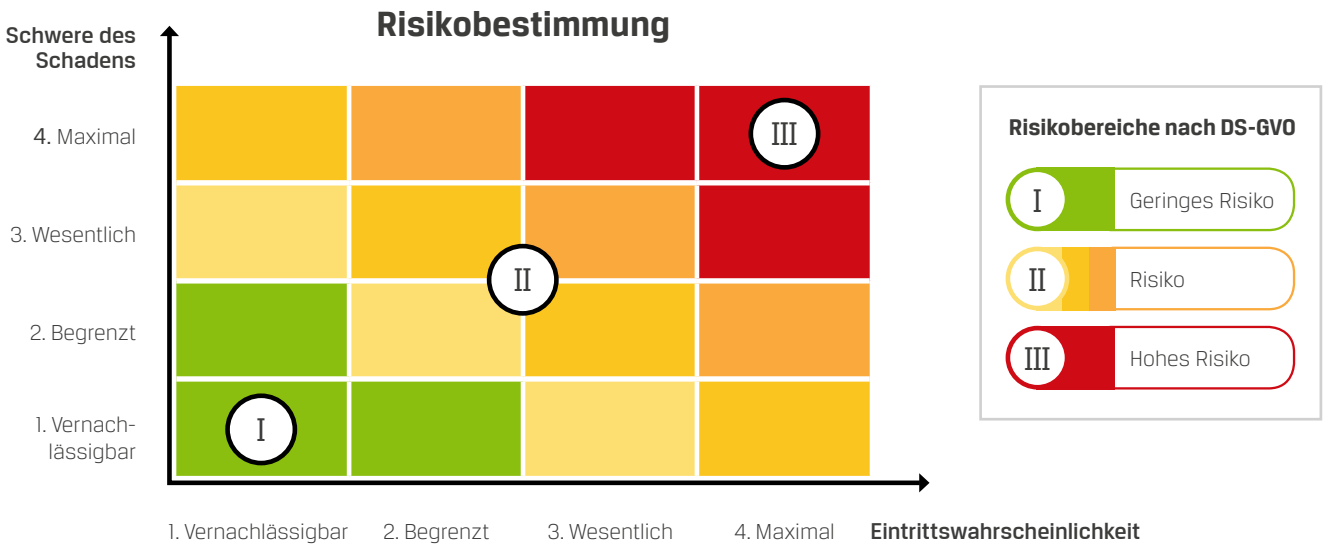
Eine vorausschauende Risikoanalyse hilft

Um Datenschutzverletzungen vorzubeugen, muss man wissen, wo sie auftreten können. Potenzielle Risiken müssen daher bestimmt und analysiert werden. Dabei sollten alle Bereiche des Unternehmens, in denen mit Daten gearbeitet wird, gründlich untersucht werden. Wo werden personenbezogene Daten erhoben? Wie werden sie verarbeitet und gespeichert?

Diese Risikoanalyse wird von der DSGVO gefordert. Insbesondere die Eintrittswahrscheinlichkeit und die Schwere eines möglichen Schadens sollen dafür berücksichtigt werden. Anhand dessen kann der **Datenschutzbeauftragte** gezielt geeignete Maßnahmen ergreifen.

Eine **Risikomatrix** kann helfen, potenzielle Risiken der Datenspeicherung zu erkennen. So wird deutlich, wo Handlungsbedarf besteht. Jedes potentielle Risiko kann anhand seiner Eintrittswahrscheinlichkeit und anhand der Schwere des Schadens genau verortet werden. Die drei Risikogruppen gering – mittel – hoch zeigen dann den Handlungsbedarf und den notwendigen Aufwand zur Sicherung an.

In Art. 32 Abs. 1 der EU-DSGVO wird dazu festgestellt: "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[.]"



Eine **vollständige Übersicht** über alle Speicherorte von personenbezogenen Daten erleichtert den Überblick und zeigt punktgenau auf, wo am dringlichsten zu handeln ist. Durch Spalten für Risiko-Quellen, Eintrittswahrscheinlichkeit und Schadenshöhe können die **ausschlaggebenden Gründe** für die Risikobewertung direkt entnommen werden. So können Risiken effektiv beseitigt werden, um zum Stichtag 24. Mai 2018 optimal vorbereitet zu sein.

Diese Sicherheitsmaßnahmen schlägt die DSGVO vor

Kernziel der DSGVO für die Verarbeitung personenbezogener Daten ist, "ein dem Risiko angemessenes Schutzniveau zu gewährleisten" (Art. 32 Abs. 1). Nach der Risikoanalyse müssen dementsprechend Schutzmaßnahmen getroffen werden, die einerseits angemessen sind und andererseits Sicherheit garantieren können.

Glücklicherweise gibt die DSGVO auch konkrete Hinweise, wie weitreichend Sicherheitsmaßnahmen für sensible Daten sein sollen. Ebenfalls in Art. 32 Abs. 1 heißt es dazu: "[D]iese Maßnahmen schließen [...] ein: [...] die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten". Beide Verfahren können also für DSGVO-konforme Sicherheit angewendet werden.

Um personenbezogene Datensätze zu pseudonymisieren, werden Namen durch **zufällige Zahlencodes** ersetzt und der Schlüssel in einer **Mastertabelle** abgespeichert. Das Verfahren hat den großen Vorteil, dass es vollautomatisiert werden kann. Dafür jedoch muss die Mastertabelle jederzeit verfügbar sein und darf nicht verloren gehen oder überschrieben werden. Kritisch ist außerdem, dass nicht immer ein Name notwendig ist, um die dahinterstehende Person zu identifizieren: Beispielsweise kann anhand von Geschlecht, Geburtsdatum und Wohnort oftmals schon auf die Identität geschlossen werden. Ein **Restrisiko** bleibt also bestehen.

Verschlüsselung ist eine weitere Sicherheitsmaßnahme, die in der DSGVO empfohlen wird. Dabei sollten Daten in jedem Zustand und zu jedem Zeitpunkt der Übertragung verschlüsselt werden.

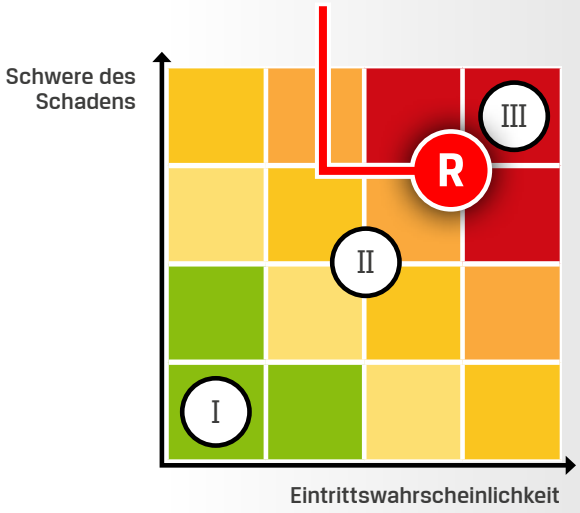
Ein gutes Qualitäts-merkmal für Verschlüsselungen sind freiwillige **Herstellerzertifizierungen wie z.B. FIPS 197 oder 140 – Level3**. Diese garantieren einen bestimmten Sicherheitsstandard und werden zukünftig im Rahmen der DSGVO eine wichtigere Rolle als Nachweis spielen.

Sind personenbezogene Daten sicher verschlüsselt – 256-Bit-AES-Verschlüsselung ist Stand der Technik – , können sie selbst bei einem Datendiebstahl oder einer Datenpanne nicht genutzt werden. Dadurch entfällt die Informationspflicht an Betroffene oder eine öffentliche Bekanntmachung, da keine Gefahr besteht. Die zuständige Aufsichtsbehörde muss dennoch benachrichtigt werden.

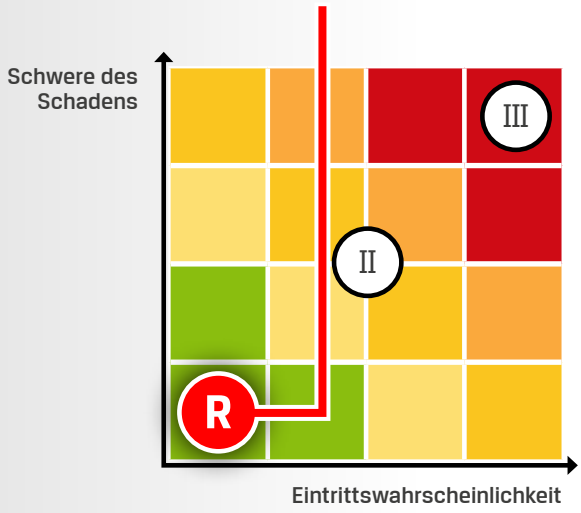
Verschlüsselte USB-Sticks jederzeit, an jedem Ort: Kingston Technology

Der bereits erwähnten Studie zufolge gehen Unternehmen, die personenbezogene Daten auf unverschlüsselten USB-Sticks speichern, ein hohes Risiko ein, da diese oftmals verloren gehen, gestohlen werden oder unauffindbar sind. Das Risiko ist hier insgesamt als hoch zu bewerten, da sowohl Eintrittswahrscheinlichkeit als auch die potenzielle Schwere des Schadens als hoch angesehen werden können. Beide lassen sich durch den Einsatz von verschlüsselten USB-Sticks signifikant senken, so dass das Gesamtrisiko als „vernachlässigbar" eingestuft werden kann.

Datenrisiko USB-Stick ohne Verschlüsselung



Datenrisiko USB-Stick mit Verschlüsselung



Kingston Technology bietet mit den Produktserien DataTraveler DTVP3.0 und DT4000G2 und den IronKey D300 und S1000 verschiedene USB-Sticks an, die o.g. höchsten Sicherheitsansprüchen genügen. Die gespeicherten Daten sind hundertprozentig verschlüsselt und ein komplexer Passwortschutz mit Mindestanforderungen schützt gegen unbefugten Zugang. Nach 10 ungültigen Anmeldeversuchen ist beispielsweise ein Zugriff auf die Daten nicht mehr möglich.

Die USB-Sticks von Kingston sind nach dem Sicherheitsstandard **AES-256** im XTS Modus verschlüsselt. Dieser Algorithmus entspricht heutigen Sicherheitsstandards. Zertifizierungen gemäß **FIPS 197** und **FIPS 140-2** sorgen dafür, dass Ihre Daten auch im Fall der Entwendung oder des Verlustes absolut sicher sind. Die Versionen DataTraveler 4000G2, IronKey D300 und IronKey S1000 bieten zudem einen physischen Schutz vor Manipulation gemäß FIPS 140-2. Kingston bietet für einige seiner USB-Sticks (DTVP3.0, DTVP3.0AV, DT4000G2 mit Management und D300) zudem ein **Personalisierungsprogramm** an, mit dem z.B. über Seriennummern und Produkt IDs die Einbindung in eine Endpoint-Management Lösungen vorgenommen werden kann oder die Anzahl der erlaubten Passworteingabeversuche festgelegt werden können.

Um auch Management-Lösungen für die verschlüsselten USB-Sticks anbieten zu können, ist Kingston Technology eine Partnerschaft mit **DataLocker** eingegangen. DataLocker stellt für Kingstons verschlüsselte DataTraveler und IronKey USB-Laufwerke die Software-Programme SafeConsole und Enterprise Management System (EMS) zur Verfügung, über welche die USB Sticks einfach zentral im Unternehmen verwaltet werden können.

Kingstons DataTraveler Vault Privacy 3.0 und DataTraveler 4000 G2 sind als Managed Versionen (optionales Management) erhältlich, und unterstützen beide die zentrale Verwaltung über SafeConsole von DataLocker. IronKeys D300 und S1000 gibt es ebenfalls als Managed Modelle und beide unterstützen die IronKey EMS von DataLocker.

Mit diesen Lösungen können **Compliance-Anforderungen** leichter erfüllt werden und Mitarbeitern **mehr Support** zur Verfügung gestellt werden, z.B. Remote Password Reset oder automatische Anti-Maleware Scanner. Sie vereinfachen ebenso die Einhaltung von umfassenden Sicherheitsrichtlinien, da sie Systemadministratoren die einfache Kontrolle über alle Laufwerke eines Unternehmens ermöglichen.

Sollte also ein verschlüsselter USB-Stick von Kingston verloren gehen, bedeutet dies nicht automatisch einen Datenvorfall. Damit eliminieren verschlüsselte mobile Speichermedien ein bekanntes, oft unterschätztes und vernachlässigtes Sicherheitsrisiko in Unternehmen. Schließen Sie eine kleine, aber gefährliche Sicherheitslücke durch den Einsatz von verschlüsselten USB-Sticks und **vermeiden Sie so einen Datenschutzverstoß gemäß DSGVO**.

Haben Sie noch Fragen?

Dann zögern Sie nicht,
uns zu kontaktieren:

+44 (0) 1932 738888

EncryptedUSB@kingston.eu

www.kingston.com

Kingston Technology Europe Co LLP und Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, England. Tel: +44 (0) 1932 738888, Fax: +44 (0) 1932 785469.

Dieses Whitepaper wurde von der B2B Media Group GmbH im Auftrag von Kingston Technology Europe Co LLP und Kingston Digital Europe Co LLP erstellt.
http://www.b2bmg.de / kontakt@b2bmg.de