Kensington The Professionals' Choice™

Warum eine Richtlinie für physische Sicherheit **bei der DSGVO-Compliance unerlässlich ist**

Haftungsausschluss: *Keine der in diesem Dokument enthaltenen Informationen sind als Rechtsberatung anzusehen. Organisationen sollten im Hinblick auf die Einhaltung der Datenschutz-Grundverordnung und aller sonstigen anwendbaren Gesetzen und Bestimmungen ihren Rechtsbeistand konsultieren.*

DATEN GESCHÜTZT

Inhalt

WARUM EINE RICHTLINIE FÜR PHYSISCHE SICHERHEIT **BEI DER DSGVO-COMPLIANCE UNERLÄSSLICH IST**

Über **dieses Dokument**

*Dieses Whitepaper bietet Ihnen **einen Überblick darüber, welche Ziele die DSGVO verfolgt** und welche Probleme sie für Organisationen mitbringt.*

WARUM EINE RICHTLINIE FÜR PHYSISCHE SICHERHEIT **BEI DER DSGVO-COMPLIANCE UNERLÄSSLICH IST**

Der Zweck dieses Papiers besteht darin, Ihnen eine Einführung in die Datenschutz-Grundverordnung der EU (DSGVO) und deren Auswirkungen auf unterschiedliche Unternehmen zu vermitteln, so dass Sie bereits vor Inkrafttreten der Regelungen im Mai 2018 eine angemessene Richtlinie für physische Sicherheit in Ihrem eigenen Unternehmen entwickeln können.

Was genau ist die DSGVO? Die DSGVO verlangt von Organisationen, dass sie sachgerechte Sicherheitsmethoden für elektronische und papierbasierte Daten anwenden und im Falle eines Verstoßes die betroffenen oder potenziell betroffenen Personen hierüber in Kenntnis setzen. Der Geltungsbereich der DSGVO erstreckt sich weltweit auf alle Organisationen (ungeachtet ihres tatsächlichen geografischen Standorts), die personenbezogene Daten über Personen in der EU besitzen oder verarbeiten. Die Anforderungen der DSGVO gelten sowohl für elektronische als auch papierbasierte Daten. Grundsätzlich sollten alle Organisationen den DSGVO-Anforderungen Rechnung tragen, wenn sie aus der EU stammende personenbezogene Daten handhaben.

Der Schutz von Daten gegen Hacking und Malware ist in vielen Organisationen zu Recht eine Priorität. Dabei wird jedoch oft vergessen, auch für die physische Sicherheit der IT-Hardware zu sorgen. Mehr als die Hälfte aller Organisationen haben keine physischen Schlösser an ihren IT-Geräten[1] . Damit laufen sie Gefahr, gegen die DSGVO zu verstoßen, und setzen Datensubjekte dem Risiko von Betrug und Identitätsdiebstahl aus. In diesem Zusammenhang ruft Kensington Organisationen dazu auf, ihre Sicherheitsrichtlinien und -praktiken in Bezug auf elektronische Daten zu überprüfen.

Überblick

Hauptziel der DSGVO ist zwar die Stärkung der Online-Datenschutzrechte, doch auch dem Schutz der physischen Hardware kommt ein hoher Stellenwert zu.

Die DSGVO ist eine Reaktion auf ständig zunehmende Datenschutz-Herausforderungen, Sicherheitsverletzungen, Hacking und andere Formen der unrechtmäßigen Datenverarbeitung.

*Die **folgenden Bereiche der DSGVO** sind entweder neu oder schaffen mehr Rechte für Privatpersonen.*

1

Datenübertragbarkeit und das Recht auf Vergessen

- Natürliche Personen haben jetzt das Recht, ihre personenbezogenen Daten von einer Organisation auf die nächste zu übertragen.
- Personenbezogene Daten müssen in einem strukturierten und maschinenlesbaren Format bereitgestellt werden.
- Eine Person kann verlangen, dass ihre personenbezogenen Daten gelöscht oder entfernt werden.

2

Datenbestand

- Die Verarbeitung personenbezogener Daten muss nicht mehr den örtlichen Behörden gemeldet werden.
- Organisationen obliegt die Verantwortung, über alle Verarbeitungstätigkeiten, für die sie verantwortlich sind, Buch zu führen.

3

Folgenabschätzungen in Bezug auf Datenschutz und -sicherheit

- Folgenabschätzungen in Bezug auf Datenschutz und -sicherheit sind eine Methode, hohe Datenschutzrisiken für natürliche Personen zu identifizieren.
- Sicherheitsanforderungen und -empfehlungen sollten auf einer Risikobewertung basieren.

4

Meldung von Datenschutzverletzungen

- Alle Datenschutzverletzungen müssen der Aufsichtsbehörde gemeldet werden.
- Die von der Datenschutzverletzung betroffenen Personen müssen ebenfalls informiert werden.

5

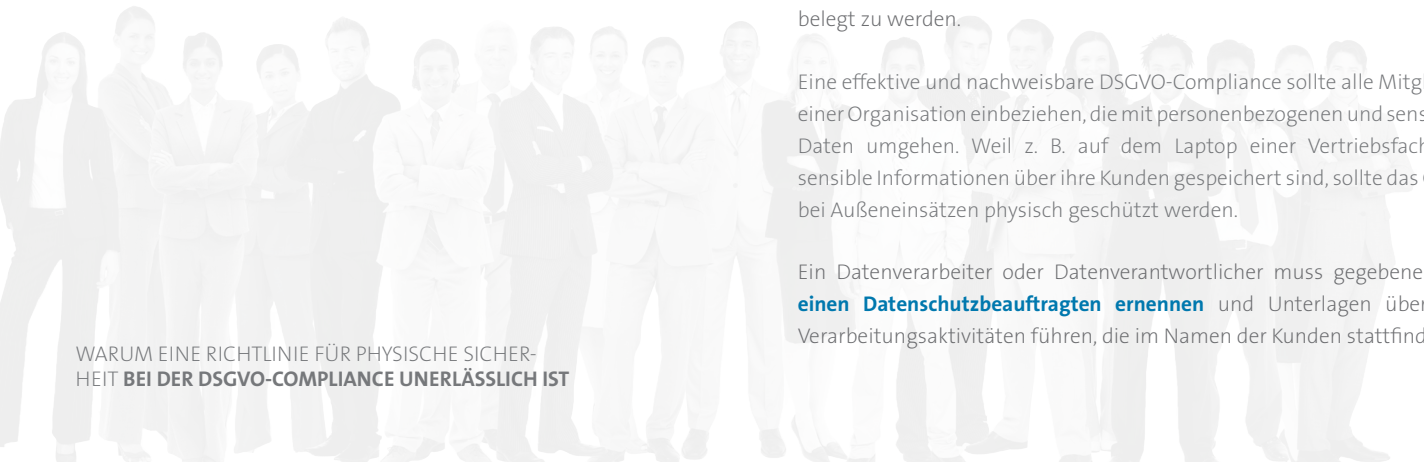
Daten-Governance und Rechenschaftspflicht

- Organisationen müssen außerdem in der Lage sein, die Einhaltung der DSGVO nachzuweisen.

WARUM EINE RICHTLINIE FÜR PHYSISCHE SICHERHEIT **BEI DER DSGVO-COMPLIANCE UNERLÄSSLICH IST**

Wer ist **betroffen?**

Jede Organisation, die Daten über EU-Bürger verarbeitet (auch wenn sie ihren Sitz außerhalb der EU hat), muss die Anforderungen der DSGVO erfüllen, und ihre Regelungen betreffen jeden, der mit diesen Daten zu tun hat.



Die DSGVO gilt für Organisationen mit Sitz in der EU und außerhalb der EU, die Daten über lebende Einwohner oder Bürger der EU besitzen oder verarbeiten.

Die DSGVO betrifft vor allem:

Datenverantwortliche: Personen mit Verantwortung dafür, wie und warum persönliche Daten verarbeitet werden

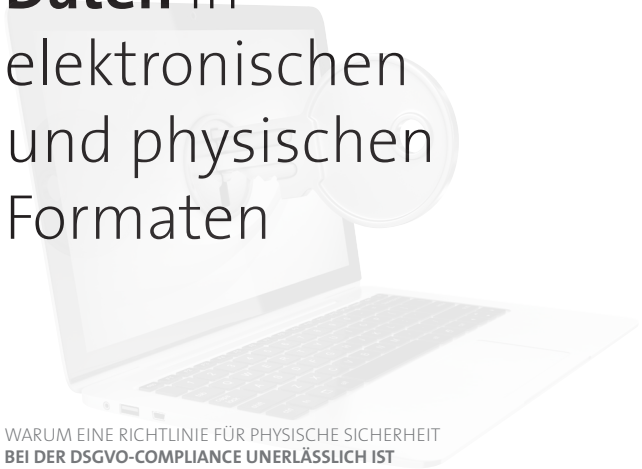
Datenverarbeiter: Personen, die im Auftrag des Datenverantwortlichen handeln

Es ist die Verantwortung dieser beiden Personen sicherzustellen, dass ihre Kunden jegliche Aspekte der DSGVO einhalten, um nicht mit Geldbußen belegt zu werden.

Eine effektive und nachweisbare DSGVO-Compliance sollte alle Mitglieder einer Organisation einbeziehen, die mit personenbezogenen und sensiblen Daten umgehen. Weil z. B. auf dem Laptop einer Vertriebsfachkraft sensible Informationen über ihre Kunden gespeichert sind, sollte das Gerät bei Außeneinsätzen physisch geschützt werden.

Ein Datenverarbeiter oder Datenverantwortlicher muss gegebenenfalls **einen Datenschutzbeauftragten ernennen** und Unterlagen über alle Verarbeitungsaktivitäten führen, die im Namen der Kunden stattfinden.

Die DSGVO betrifft **personenbezogene Daten** und **sensible personenbezogene Daten** in elektronischen und physischen Formaten



Bevor Sie eine Compliance-Richtlinie für Ihre Organisation entwickeln, sollten Sie feststellen, auf welche Arten von Daten die DSGVO Anwendung findet.

Der Geltungsbereich der DSGVO umfasst alle Informationen über eine identifizierbare Person. Daten fallen hierbei in eine von zwei Kategorien:

Personenbezogene Daten sind z. B. Angaben wie eine E-Mail-Adresse oder Postanschrift oder auch Informationen, die als Online-Kennung dienen können, wie eine IP-Adresse.

Sensible personenbezogene Daten sind persönlichere Informationen wie ethnische Herkunft, politische Überzeugungen, Religion und medizinische Daten. Generell müssen Organisationen triftigere Gründe haben, solche Informationen zu verarbeiten, als bei „normalen" personenbezogene Daten.

Die DSGVO betrifft von Organisationen verarbeitete personenbezogene Daten in **elektronischen und physischen Formaten** (z. B. Papierdokumente).

Ein Rahmenwerk für die **DSGVO-Compliance**

Durch Überprüfen dieser drei Komponenten (Personen, Prozesse und Technologien) werden Organisationen in der Lage sein, einen klaren Rahmen für ihre Datenschutzrichtlinie abzustecken, was ihnen wiederum helfen wird, Konformität mit allen Aspekten der DSGVO zu erreichen.

WARUM EINE RICHTLINIE FÜR PHYSISCHE SICHERHEIT
BEI DER DSGVO-COMPLIANCE UNERLÄSSLICH IST

In Organisationen müssen drei Hauptbereiche überprüft werden, um DSGVO-Compliance zu erreichen:

Mitarbeiter: Es ist absolut wesentlich, dass Mitarbeiter Verantwortung für die Daten übernehmen, die sie innerhalb der Organisation verarbeiten. Eine Organisation muss allen Mitarbeitern klare Regeln für die ordnungsgemäße Handhabung elektronischer Daten im Unternehmen geben. Mit diesen Regeln werden die Anforderungen der DSGVO im Hinblick auf die Handhabung aller Daten umgesetzt. So könnten Sie beispielsweise klare Bestimmungen einführen, die die Verwendung sensibler Daten auf Firmenlaptops und das Verfahren zum Löschen von Daten regeln.

Prozesse: Dies bezieht sich auf die Prozesse innerhalb der Organisation, beispielsweise Verfahren zum Verarbeiten und Speichern von Kundendaten. Es ist wichtig, dass Unternehmen all ihre gegenwärtigen Datenverarbeitungsprozesse überprüfen. Werden dabei Lücken und Schwächen identifiziert, muss das Unternehmen einen Rahmenplan entwickeln, um diese Bereiche zu stärken oder gegebenenfalls zu ersetzen, so dass die Anforderungen der DSGVO erfüllt sind.

Technologie: Aktuelle IT-Funktionen und -Anforderungen sollten ebenfalls überprüft und vor Mai 2018 entsprechend geändert werden. Es obliegt jedem einzelnen Unternehmen sicherzustellen, dass alle nicht vollständig konformen Systeme entweder verbessert oder ersetzt werden, um potenzielle Geldbußen bei Inkrafttreten der DSGVO zu vermeiden.

Warum **physische Sicherheit** wichtig ist

*Online- und softwarebasierte Bedrohungen sind zwar wichtige Anliegen für Organisationen, doch wäre es ein Fehler anzunehmen, dass **physische Sicherheitsrisiken** der Vergangenheit angehören.*

Nachdem wir die Anforderungen der DSGVO an Unternehmen betrachtet haben, ist es nun an der Zeit, über die Sicherheit physischer Geräte innerhalb von Organisationen nachzudenken – ein wichtiges Anliegen für Unternehmen im Vorfeld der DSGVO.

Nach Online-Bedrohungen und der unbeabsichtigten Enthüllung von Daten sind **tragbare Geräte** und **physischer Verlust** die größten Quellen von Datenschutzverstößen[2]:

Jeden Tag werden durchschnittlich über **5 Millionen Datensätze verloren oder gestohlen**[3], und mehr als **ein Drittel aller Unternehmen hat keine Richtlinie für die physische Sicherheit** ihrer Laptops, mobilen Geräte und anderen elektronischen Bestände.[4]

Angesichts der hohen Geldstrafen, die mit der DSGVO anstehen, einer zunehmend mobilen Belegschaft und der steigenden Nutzung von Hot-Desking ist der physische Schutz von Laptops und mobilen Geräten eine sinnvolle Vorsichtsmaßnahme, sowohl am Arbeitsplatz als auch unterwegs. Die physische Sicherung von Geräten mit einem Schloss ist eine schnelle und einfache Art, Diebstahl zu verhindern – und dabei ausgesprochen wirksam.

Kensington bietet eine umfassende Auswahl an **Schließlösungen** für eine breite Vielfalt an Laptops, einschließlich Geräten ohne Sicherheits-Slot. Die Taschen der SecureTrek™ Serie lassen sich physisch an einem feststehenden Gegenstand sichern, z. B. in Flughäfen, Hotels und Messen.

WARUM EINE RICHTLINIE FÜR PHYSISCHE SICHERHEIT **BEI DER DSGVO-COMPLIANCE UNERLÄSSLICH IST**

Physische Sicherheit ist immer noch die Ursache **vieler gängiger Sicherheitsverstöße**

WARUM EINE RICHTLINIE FÜR PHYSISCHE SICHERHEIT **BEI DER DSGVO-COMPLIANCE UNERLÄSSLICH IST**

Unter 697 Datensicherheitsvorfällen, die von der britischen Datenschutzbehörde Information Commissioner's Office (ICO) erfasst wurden, betrafen 6 % den Diebstahl eines unverschlüsselten Geräts. Das Speichern von Daten an einem ungeschützten Ort und der Diebstahl der einzigen Kopie verschlüsselter Daten kamen für weitere 3,5 % auf[5].

Im **Finanzsektor** gehen 25 % aller Sicherheitsverstöße auf verlorene oder gestohlene Geräte zurück – dies ist die häufigste Ursache von Datenlecks und aufgrund des hohen Volumens sensibler Daten, die gespeichert und verarbeitet werden, ein besonders verlockendes Ziel für Angreifer.[6]

Im **Gesundheitswesen** ist physischer Verlust oder Diebstahl die wichtigste Ursache von Sicherheitsvorfällen und machte 32 % von über 100.000 untersuchten Fällen in 82 Ländern aus.[7]

Aktuelle IT-Funktionen und -Anforderungen sollten ebenfalls überprüft und vor Mai 2018 entsprechend geändert werden. Es obliegt jedem einzelnen Unternehmen sicherzustellen, dass alle nicht vollständig konformen Systeme entweder verbessert oder ersetzt werden, um potenzielle Geldbußen bei Inkrafttreten der DSGVO zu vermeiden.

Nutzer- Kooperation ist wesentlich für DSGVO-Compliance

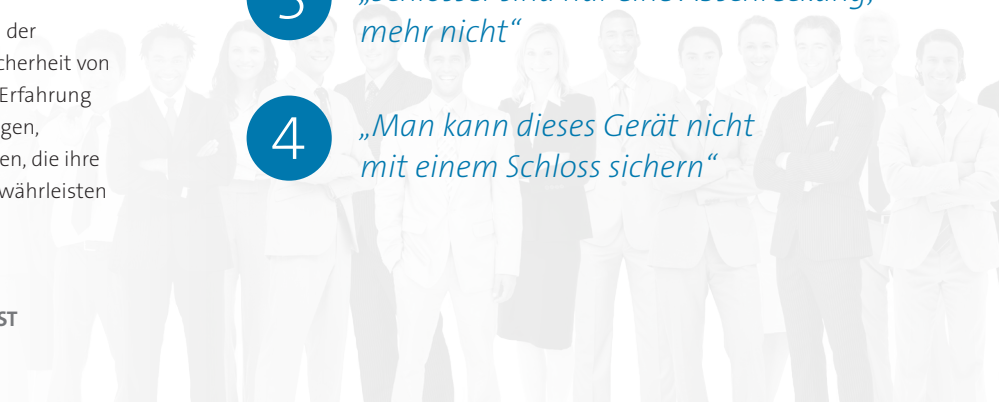
Wenn wir also wissen, dass die physische Sicherheit maßgeblich für die Informationssicherheit ist, dann müssen wir uns die Frage stellen: Was können Unternehmen diesbezüglich tun?

Kensington ist der Erfinder des Laptopschlosses und der weltweite Markführer, wenn es um die physische Sicherheit von IT-Hardware geht. Kensington besitzt über 35 Jahre Erfahrung sowie umfassendes Know-how über die Anforderungen, Wünsche und Herausforderungen von Organisationen, die ihre Werte schützen und Konformität mit der DSGVO gewährleisten möchten.

WARUM EINE RICHTLINIE FÜR PHYSISCHE SICHERHEIT **BEI DER DSGVO-COMPLIANCE UNERLÄSSLICH IST**

Aufgrund dieser Erkenntnisse sehen wir vier wesentliche Einwände und Hindernisse, die der effektiven physischen Sicherheit von Organisationen im Wege stehen:

1. *„Wir arbeiten in einer sicheren Umgebung“*
2. *„Wir verschlüsseln unsere Daten und speichern sie in der Cloud“*
3. *„Schlösser sind nur eine Abschreckung, mehr nicht“*
4. *„Man kann dieses Gerät nicht mit einem Schloss sichern“*



Hindernisse für die DSGVO-Compliance

WARUM EINE RICHTLINIE FÜR PHYSISCHE SICHERHEIT **BEI DER DSGVO-COMPLIANCE UNERLÄSSLICH IST**

„Wir arbeiten in einer sicheren Umgebung“

Überwachungskameras, Mitarbeiterausweise und Sicherheitskräfte können bedeuten, dass man sich sicherer und weniger gefährdet fühlt. Tatsache ist allerdings, dass 58 % der Laptops aus Büros gestohlen werden und 85 % der IT-Manager dabei internen Diebstahl vermuten.[8] Daten sind in Gefahr, sobald der Laptop entwendet wurde – vor allem, weil nur 3 %[9] je wiedergefunden werden. Mit Laptop-Schlössern verhindern Sie opportunistische Diebstähle und vermeiden den Zeit- und Kostenaufwand, der mit der Verfolgung des Diebs und dem Ersetzen des Laptops verbunden ist, ganz zu schweigen von den potenziellen Geldbußen infolge der DSGVO.

„Wir verschlüsseln unsere Daten und speichern sie in der Cloud“

Datenverschlüsselung ist keine Hilfe, wenn die Daten auf einem gestohlenen Gerät nicht anderswo gesichert sind. Selbst wenn Benutzer keine Daten auf ihren Festplatten speichern, ist der Produktivitätsverlust für den Mitarbeiter, dem sein wichtigstes Arbeitsgerät fehlt, ein erheblicher Faktor. Gehen Sie einmal mit offenen Augen durch Ihr Büro. Wie leicht wäre es für einen Kurier, ein Gerät mitzunehmen? 49 % kleiner und mittlerer Unternehmen brauchen 2 bis 4 Tage, um einen verlorenen oder gestohlenen Laptop zu ersetzen.[8]

„Schlösser sind nur eine Abschreckung, mehr nicht“

Laptopschlösser sollen vor allem opportunistische Diebe abschrecken, helfen aber auch sehr effektiv, Diebstähle zu verhindern. Laut Daten von IDC sagen 52 % der IT-Manager, die Laptop-Diebstahl erlebt haben, dass der Diebstahl durch ein Schloss hätte verhindert werden können.[8]

Hindernisse für die DSGVO-Compliance

„Man kann dieses Gerät nicht mit einem Schloss sichern“

Geräte werden immer flacher und verfügen oft nicht mehr über den standardmäßigen Kensington Security Slot™. Allerdings bedeutet das nicht, dass es keine Möglichkeit gibt, solche Geräte physisch zu sichern. Auch Geräte ohne Sicherheits-Slot lassen sich mit einem Schloss versehen, um opportunistische Diebstähle zu verhindern. Kensington bietet eine umfassende Auswahl an Lösungen für verschiedenste Geräte:

MicroSaver® 2.0 und ClickSafe® 2.0

Für Geräte mit dem gängigen Kensington Security Slot™ (90 % aller Business-Geräte).

Kensington Security Slot™ an Laptop und Desktop

MicroSaver® 2.0 Schloss, direkt in Security Slot gesteckt

ClickSafe® 2.0 Schloss, mit ClickSafe Anchor befestigt

N17 für Dell-Geräte 2017

Für Geräte mit dem Wedge Security Slot (z. B. Dell Latitude Modelle 2017 und später sowie ausgewählte andere Geräte).

Wedge Security Slot

Laptop an feststehendem Gegenstand befestigt

NanoSaver™ Laptopschloss mit Schlüssel

Für Geräte mit dem Kensington Nano Security Slot™ (ultraflache Geräte).

Kensington Nano Security Slot™

NanoSaver™ Laptopschloss mit Schlüssel

Sicherungslösungen für Microsoft Surface™

Spezifische Schlösser für Surface™ Pro, Surface™ Book und Surface™ Studio.

Schloss mit Schlüssel für Surface™ Pro

Schließsystem für Surface™ Studio

Sicherungsriegel für 13.5" Surface™ Book

Laptop Locking Station 2.0

Für Geräte ohne Sicherheits-Slot (z. B. Surface™ Laptop und MacBook Pro®).

Laptop Locking Station mit MacBook Pro®

Finden Sie Ihre ideale Sicherungslösung für Laptops und andere Geräte:

www.kensington.com/lockselector.com

DSGVO: 6 entscheidende Punkte

1. Ernennen Sie bei Bedarf einen Datenschutzbeauftragten

Dieser Beauftragte muss umfassend mit den Verpflichtungen der Organisation im Hinblick auf die DSGVO vertraut sein und gründliche Kenntnis davon haben, welche Daten in Ihrer Organisation als „personenbezogen" gelten, wo sie aufbewahrt werden, wer Zugang zu ihnen hat, wie eventuelle Sicherheitsverstöße erkannt werden und wem diese zu melden sind. **Der Datenschutzbeauftragte muss kein Mitarbeiter sein – Sie können diese Funktion auslagern.**

2. Überprüfen Sie Ihre Systeme

Überprüfen Sie alle Verträge, Technologie-Support-Leistungen, Verfahren und Tools in Zusammenhang mit der Verarbeitung, Handhabung, Speicherung und Löschung von Daten, so dass Sie in der Lage sind, änderungsbedürftige Schwachstellen und Lücken zu identifizieren.

3. Entwickeln Sie eine Strategie

Entwickeln Sie eine neue Strategie, die volle Konformität mit der DSGVO gewährleistet. Diese Strategie kann bedeuten, dass Sie in neue Technologie investieren, Personalverfahren und Verantwortung für die Datenverarbeitung anpassen sowie neue Rollen innerhalb der Organisation schaffen müssen.

DSGVO: 6 entscheidende Punkte

4. Implementieren Sie eine neue Richtlinie

Der nächste Schritt in Richtung DSGVO-Compliance besteht darin, Ihren Plan auf allen Ebenen der Organisation in die Tat umzusetzen. Investieren Sie in neue Technologien und Systeme, die am Arbeitsplatz benötigt werden, und veröffentlichen Sie einen informativen Leitfaden zur Datenhandhabung und -verarbeitung.

5. Mitarbeiterengagement

Führen Sie Ihre neue, für alle Mitarbeiter geltende Daten-Compliance-Richtlinie ein; stellen Sie allen Mitarbeitern Schulungen, Informationen und Leitfäden zur Verfügung, damit sie umfassend darüber informiert sind, welche Veränderungen stattfinden und inwieweit auch sie dafür verantwortlich sind, dass das Unternehmen die Anforderungen der DSGVO erfüllt.

6. Überprüfen und verbessern

Nachdem Sie Ihren DSGVO-Compliance-Plan eingeführt haben, sollten Sie Überprüfungen und Verbesserungen vornehmen, bevor die Verordnung in Kraft tritt. Indem Sie ggf. erforderliche Verbesserungen rechtzeitig vor Inkrafttreten der DSGVO identifizieren, kann sich Ihr Unternehmen bis Mai 2018 erfolgreich und effizient auf die Veränderungen einstellen und volle Konformität sicherstellen.

Lösungen

Laptop- und Geräteschlösser sind die ideale Antwort für Organisationen, die gewährleisten möchten, dass ihre Mitarbeiter eine Richtlinie für die Sicherheit physischer Geräte einhalten und dass ihr Risiko potenzieller Sicherheitsverstöße möglichst gering bleibt. Durch zusätzliche Lösungen lässt sich dieses Risiko sowohl innerhalb als auch außerhalb des Büroumfelds weiter reduzieren.

SecureTrek™ Taschen
Die Trolleys, Taschen und Rucksäcken der SecureTrek™ Serie lassen sich zum Schutz vor Diebstahl – beispielsweise in Flughäfen, Hotels und Messen – an einem feststehenden Gegenstand sichern.

Sichtschutzfilter
„Visual Hacking" ist einfach, geht schnell und bleibt oft unbemerkt.[10] Ein Sichtschutzfilter reduziert den Betrachtungswinkel des Bildschirms und damit das Risiko.

USB-Port-Schlösser
System-Administratoren verhindern damit die Verwendung von USB-Ports und reduzieren das Risiko, dass Benutzer unbefugt Daten kopieren oder Malware in das System hochladen.

Ladekabinette
Eine schnelle und einfache Lösung zum Laden, Synchronisieren und Sichern mehrerer Tablets und ultraflacher Laptops.

VeriMark™ Fingerabdruckverschlüsselung
Unterstützt eine einfache, schnelle und sichere biometrische Anmeldung bei Windows Hello™ und ist kompatibel mit Services, die Zwei-Faktor-Authentifizierung verlangen. Schützt vor unbefugtem Zugriff und verbessert die Online-Sicherheit.

Quellen

1. Kensington Umfrage zu IT-Sicherheit und Laptop-Diebstahl, August 2016
2. 2016 Data Breaches - Privacy Rights Clearinghouse
3. Breach Level Index, September 2017
4. Kensington Umfrage zu IT-Sicherheit und Laptop-Diebstahl, August 2016
5. Information Commissioner's Office: https://ico.org.uk/action-weve-taken/data-security-incident-trends
6. Financial Services Breach Report, Bitglass, 2016
7. Verizon Data Breach Investigations Report 2016
8. IDC Executive Brief 2010: Laptop Theft: The Internal and External Threat
9. IDC White Paper 2007: The Threat of Theft and Loss of Laptops for the SME
10. Ponemon Institute: Visual Hacking Experiment, 2015

Kensington®

kensington.com

WEITERE INFORMATIONEN ERHALTEN SIE VON:

Michael Schnaller
Key Account Manager
michael.schnaller@kensington.com
+49 (0)163 3887028

Johann Ozuna
Key Account Manager
johann.ozuna@kensington.com
+49 (0)163 3887003

Tobias Kostros
Key Account Manager
tobias.kostros@kensington.com
+49 (0)163 3887009

The Professionals' Choice™