Kensington The Professionals' Choice™

DSGVO-Konformität: Physischer Geräteschutz als unerlässliche Sicherheitslösung für mehr Datenschutz

DSGVO KONFORM*

Ein Überblick

Das Hauptziel der DSGVO ist zwar die Stärkung der Datenschutzrechte im Onlinebereich, doch auch der physischen Hardwaresicherheit muss eine bedeutende Rolle eingeräumt werden.

Die DSVGO befasst sich dabei im Kern mit den ständig wachsenden Herausforderungen zum Schutz der Daten und Privatsphäre, von Sicherheitsverletzungen, Hacking und anderen Formen der unrechtmäßigen Datenverarbeitung.

Diese Kernthemen kennzeichnen die spezifischen Bereiche der DSGVO, die eines gemeinsam haben, die Einzelperson in ihren Rechten zu stärken.

Kensington®

Mit diesem Dokument möchten wir Ihnen eine Einführung in die Datenschutz-Grundverordnung der EU (DSGVO) und deren Auswirkungen auf unterschiedliche Unternehmen geben, damit Sie eine angemessene Richtlinie zum physischen Schutz Ihrer Geräte im eigenen Unternehmen entwickeln können.

Die **DSGVO** verlangt von Organisationen, dass sie solide 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. Alle Organisationen sollten den DSGVO-Anforderungen Rechnung tragen, sobald sie aus der EU stammende personenbezogene Daten verarbeiten.

Der Schutz von Daten gegen Hacking und Malware hat in vielen Organisationen zu Recht oberste 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 betroffene Personen dem Risiko von Betrug und Identitätsdiebstahl aus. Angesichts der potenziellen Geldstrafen von bis zu **20 Mio. €** bzw. **4 % des gesamten weltweiten Jahresumsatzes des Unternehmens** ruft Kensington Organisationen dazu auf, ihre physischen Sicherheitsrichtlinien in Bezug auf elektronische Daten zu überprüfen.

Wer und was fällt in den Geltungsbereich der DSGVO?

Jede Organisation, die Daten über EU-Bürger verarbeitet, ungeachtet, ob deren Sitz außerhalb der EU ist, unterliegt der DSVGO und deren Anforderungen. Betroffen ist hiervon jeder, der mit diesen Daten arbeitet.

Im Januar 2019 verhängte die französische Datenschutzbehörde gegen Google eine Strafe von 50 Mio. € wegen Verstößen gegen die DSGVO, weil das Unternehmen Daten nicht korrekt erhoben und keine gültige Einwilligung in die Datenverarbeitung eingeholt hatte.[2]

Dies ist ein klares Beispiel dafür, dass ein US-Unternehmen (oder jede andere Organisation von außerhalb der EU) von einer EU-Datenschutzbehörde belangt werden kann.

Die Daten im Geltungsbereich der DSGVO umfassen alle Informationen über eine identifizierbare Person und sind in zwei Kategorien zu unterteilen:

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 **elektronischer und physischer Form**.

Warum physischer Geräteschutz wichtig ist

Kensington®

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

Im Jahr 2018 waren Hacking/Malware sowie der physische Verlust von Geräten die Ursache von 41 % aller Datenschutzverstöße.[3] Im Durchschnitt sind jeden Tag mehr als **6,5 Millionen Datensätze** von Verlust oder Diebstahl[4] betroffen, und mehr als ein Drittel aller Unternehmen hat keine Richtlinie für die physische Sicherheit seiner Laptops, mobilen Geräte und anderen elektronischen Bestände.[5]

Angesichts der hohen Geldstrafen infolge der DSGVO, 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. Unser Sortiment an **Blickschutzfiltern** ist mit über 52.000 Monitor-, Laptop- und Tablet-Modellen kompatibel und kann den unbefugten Einblick in vertrauliche Daten verhindern.

Physischer Geräteschutz und DSGVO-Konformität

Kensington®

„Datensicherheit und Datenschutz sind seit jeher miteinander verbunden. Sicherheit ist Voraussetzung für den Datenschutz. Keinerlei Verpflichtung zur Gewährleistung des Datenschutzes hat wirklich Bedeutung, wenn die zu schützenden Daten von unbefugten Dritten angesehen oder gestohlen werden können.“ *James Dipple-Johnstone, Deputy Commissioner, ICO.*

Die britische Datenschutzbehörde „Information Commissioner's Office“ (ICO) verzeichnete zwischen Juli und September 2018 **4.056 Datensicherheitsvorfälle**. Über 80 % davon waren keine Cyberangriffe, sondern auf Dinge wie Geräteverlust und -diebstahl oder den unbefugten Einblick in Daten zurückzuführen.[6]

- Im November 2018 wurde ein Computer mit vertraulichen Daten über **20.000 Einwohner** aus dem Rathaus der dänischen Stadt Gladsaxe gestohlen, was laut DSGVO eine Geldbuße für die Stadt nach sich ziehen könnte.[7]
- Im August 2018 wurde ein Laptop mit unverschlüsselten personenbezogenen Daten über **37.000 Kunden** des irischen Telekom-Unternehmens Eir gestohlen.[8]
- 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.[9]
- 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.[10]

Die Kooperation der Mitarbeiter ist entscheidend für die Einhaltung der DSVGO

Wenn also der physische Geräteschutz maßgeblich für die Informationssicherheit ist, was können Unternehmen diesbezüglich tun?

Kensington ist der Erfinder des Laptopschlosses und der weltweite Marktführer, 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.

Es gibt vier wesentliche Einwände und Hindernisse, für die mangelnde Wirksamkeit des physischen Geräteschutzes in Organisationen:

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 zur Einhaltung der DSGVO überwinden

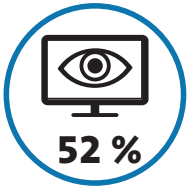
„Wir arbeiten in einer sicheren Umgebung“

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.[11] Daten sind in Gefahr, sobald der Laptop entwendet wurde – vor allem, weil nur 3 %[9] je wiedergefunden werden. Mit Laptop-Schlössern verhindern Sie Diebstähle, ersparen sich den Zeit- und Kostenaufwand, der mit der Verfolgung des Diebs und dem Ersetzen des Laptops verbunden ist, und vermeiden die potenziellen Geldbußen infolge der DSGVO.

Mobiles Arbeiten wird immer beliebter, und es kommen immer mehr hochauflösende Bildschirme zum Einsatz. Damit steigt aber auch das Risiko, dass unbefugte Beobachter Zugriff auf vertrauliche Daten erlangen. Ein verdecktes Experiment[12] in verschiedenen Arbeitsumgebungen ergab Folgendes:

„VISUAL HACKING“ IST EINFACH

In 9 von 10 Fällen war Einblick in vertrauliche Daten möglich.



COMPUTERBILDSCHIRME SIND GEFÄHRDET

Mehr als die Hälfte der Angriffe resultierte aus dem mangelnden Schutz von Bildschirmen.

BLEIBT OFT UNBEMERKT

In mehr als zwei von drei Versuchen hat niemand den Hacker bemerkt.

Hindernisse zur Einhaltung der DSGVO überwinden

„Wir arbeiten in einer sicheren Umgebung“

Blickschutzfilter sind ein wichtiger Bestandteil der Maßnahmen, die ein Unternehmen zur Erhöhung der Gerätesicherheit ergreifen sollte, vor allem im Hinblick auf die Datenschutz-Grundverordnung (DSGVO). Ein Blickschutzfilter als visuelle Barriere ist eine unerlässliche Sicherheitsvorrichtung, um vertrauliche oder personenbezogene Daten des Unternehmens zu schützen.

DSGVO KONFORM*

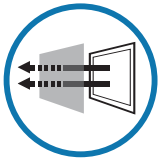
Die Vorteile von Blickschutzfiltern

Beschränkter Einblickwinkel

Touchscreen-geeignet

Leichte Anbringung

Blendschutz-Beschichtung



Blaulicht-filter

Effektiver Bildschirmschutz

* Blickschutzfilter unterstützen die DSGVO-Konformität

Unser Produktangebot umfasst mehr als 52.000 Blickschutzfilter für eine Vielzahl unterschiedlicher Hersteller, Modelle und Gerätetypen:

Bildschirme

All-in-one-Computer

Laptops

2-in-1-Hybride

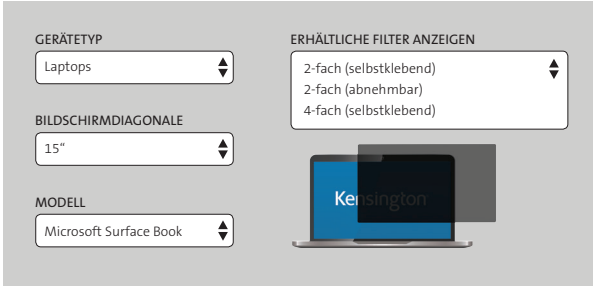
Tablets

Wir sind in der Lage, schnell auf Marktentwicklungen und Nischenanforderungen zu reagieren und fertigen auf Anfrage neue Filtermodelle.

Blickschutzfilter Konfigurator

Unser Blickschutzfilter Konfigurator macht die Wahl der richtigen Lösung zum Kinderspiel. Grenzen Sie die Auswahlmöglichkeiten ein, indem Sie den Gerätetyp, die Bildschirmdiagonale oder einfach den Modellnamen eingeben.

Weitere Informationen finden Sie unter:
www.kensington.com/blickschutz



Hindernisse zur Einhaltung der DSGVO überwinden

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

Ganz gleich, ob die Daten auf einem gestohlenen Gerät verschlüsselt sind, der Schaden ist beachtlich, wenn keine Datensicherung vorgenommen wurde. 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 % der kleinen und mittleren Unternehmen brauchen 2 bis 4 Tage, um einen verlorenen oder gestohlenen Laptop zu ersetzen.[13]

„Schlösser sind nur eine Abschreckung, mehr nicht“

Laptopschlösser sollen zum einen abschrecken und zum anderen sind sie ein wirksames Mittel, um Diebstähle zu verhindern. Laut Daten von IDC sagten 52 % der IT-Manager, die Erfahrung mit Laptop-Diebstahl haben, dass der Diebstahl durch ein Schloss hätte verhindert werden können.[13]

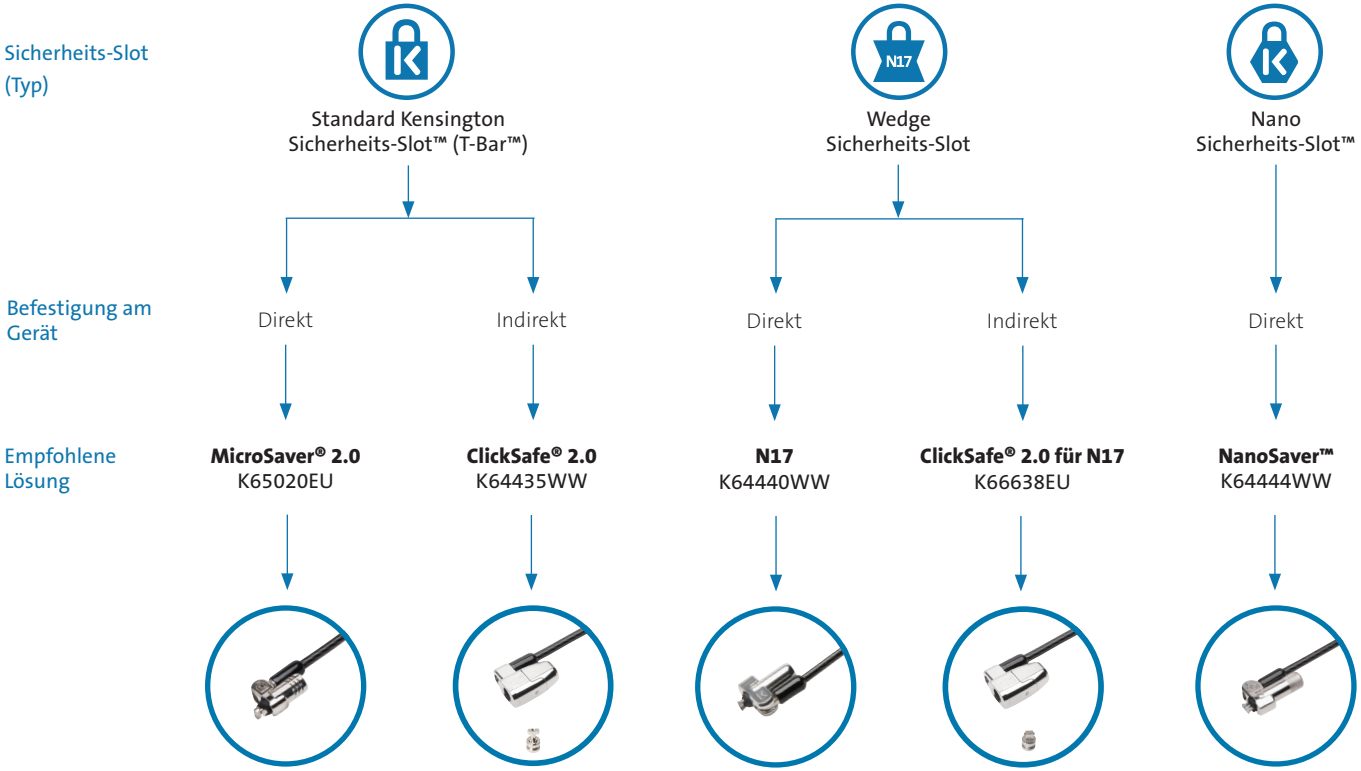
Kensington®

Hindernisse zur Einhaltung der DSGVO überwinden

„Man kann dieses Gerät nicht mit einem Schloss sichern“

Die Geräte werden immer flacher und verfügen oft nicht mehr über den standardmäßigen Kensington Sicherheits-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 Diebstähle zu verhindern. Kensington bietet eine umfassende Auswahl an Lösungen für verschiedenste Geräte: Erfahren Sie mehr unter **kensington.com/securityselector**

Kensington®



Finden Sie ganz einfach das kompatible Schließsystem unter www.kensington.com/securityselector

Kein
Sicherheits- Slot

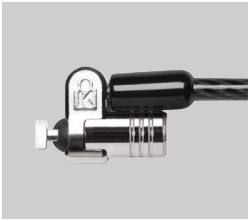
Lösungen für Surface™

Laptop Locking Stationen

Lösungen für iMac®

MicroSaver® 2.0 und ClickSafe® 2.0

Geeignet für Geräte mit dem gängigen Kensington Sicherheits-Slot™ (T-bar™), über den 90 % aller Business-Geräte weltweit verfügen.



Kensington Sicherheits-Slot™ an einem Laptop (1) oder Desktop-PC (2)

MicroSaver® 2.0 Schloss, direkt in Security Slot gesteckt (3)

ClickSafe® 2.0 Schloss, mit ClickSafe Anker befestigt (4)

Finden Sie ganz einfach das kompatible Schließsystem unter www.kensington.com/securityselector

N17 für Wedge Sicherheits-Slots

Für Geräte wie z. B. Dell Latitude Modelle 2017 und später sowie ausgewählte andere Geräte

Wedge Sicherheits-Slot

N17 Schließkopf zur direkten Befestigung am Gerät

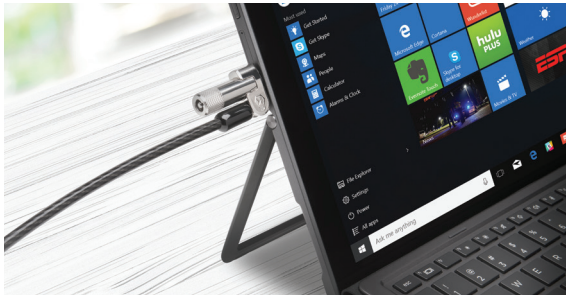
ClickSafe® 2.0 für N17 mit Sicherheitsanker

NanoSaver™ Laptopschloss mit Schlüssel

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

NanoSaver™ Sicherheits-Slot

NanoSaver™ Schließkopf



Sicherheitslösungen für Microsoft Surface™

Gerätespezifische Schlösser für Surface™ Pro, Surface™ Book, Surface™ Laptop und Surface™ Studio

SD7000 Surface™ Pro Dockingstation - K62917EU

Surface™ Pro / Go Kabelschloss K62044WW

Surface™ Book Sicherungsriegel K64821WW

Surface™ Studio Schließsystem K67976WW

Laptop Locking Stationen

Nicht-invasive Sicherheit für Laptops ohne Sicherheits-Slot, wie Surface™ Laptop und MacBook® Pro

LD5400T Thunderbolt™ 3 Dockingstation - K33476EU

LD4650P USB-C™ Dockingstation - K38400EU

Laptop Locking Station mit K-Fob™ K66635EU

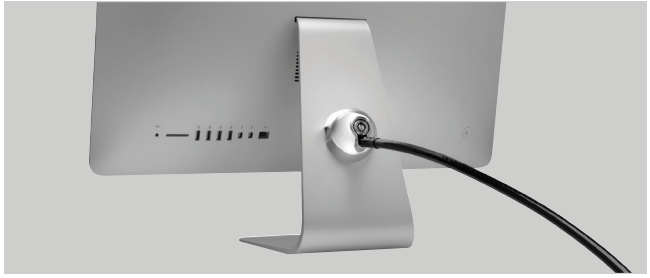
Laptop Locking Station 2.0 K64453WW

Finden Sie ganz einfach das kompatible Schließsystem unter www.kensington.com/securityselector

Sicherheitslösungen für Apple iMac®

Zwei innovative, nicht-invasive Sicherheitslösungen für den Apple iMac®

SafeDome™ montierter Sicherheitsstand für iMac® - K67822WW

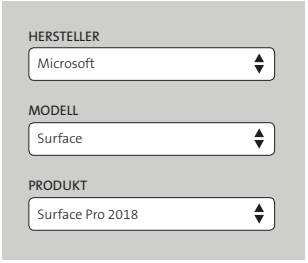


SafeDome™ Kabelschloss für iMac® - K64962EUA

Laptop Schloss Konfigurator

www.kensington.com/securityselector

Mit dem Kensington Laptop Schloss Konfigurator finden Sie ganz einfach das richtige Schloss. Wählen Sie dazu den Hersteller und das Model oder suchen Sie direkt nach dem Laptop- Model in der Auswahlliste.



Finden Sie ganz einfach das kompatible Schließsystem unter www.kensington.com/securityselector

Weitere Lösungen zur Einhaltung der DSGVO

Schließsysteme für Geräte und Blickschutzfilter helfen Unternehmen und ihren Mitarbeitern bei der Einhaltung der Compliance Richtlinien, sichern zudem die Geräte physisch und minimieren die Gefahr möglicher Sicherheitsverstöße.

Darüber hinaus bieten wir weitere Lösungen, die das Risiko sowohl innerhalb als auch außerhalb des Büroumfelds weiter reduzieren.

SecureTrek™ Taschen

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

Sicherheitskabinette

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

AES-verschlüsselte Mäuse und Tastaturen

Warum Verschlüsselung so wichtig ist
Weil drahtlose Technologien heutzutage praktisch überall eingesetzt werden, besteht oft die Annahme, dass sie sicher sein müssen. In Wirklichkeit ist eine drahtlose Verbindung jedoch ein potenzieller Schwachpunkt in einem Netzwerk, der private und vertrauliche Daten der Gefahr unbefugter Zugriffe aussetzt.

Die Schwäche drahtloser Verbindungen
Drahtlose Mäuse und Tastaturen senden Daten (über Ihre Klicks und Tastendrücke) an einen Empfänger. Ein Hacker könnte diese Informationen über die Aktivitäten des Benutzers abfangen und dadurch Zugang zu Passwörtern, Finanzdaten und anderen vertraulichen Informationen erlangen.

Der AES-Vorteil
Der Advanced Encryption Standard (AES) ist ein Verschlüsselungsstandard für elektronische Daten. AES verwandelt Klicks und Tastendrücke vor dem Senden in komplexe Codes (AES-128 z. B. verwendet 128-Bit-Schlüssel). Am anderen Ende werden diese Codes dann wieder entschlüsselt. AES wurde 2001 eingeführt und von der US-Regierung sowie anderen Ländern rund um die Welt übernommen, um vertrauliche Daten und Informationen zu schützen.

Pro Fit® flaches, kabelloses Desktop Set - K75230DE

Pro Fit® kabellose mobile Maus
K72452WW

Pro Fit® kabellose Full-Size-Maus
K72370EU

Pro Fit® kabellose Mid-Size-Mäuse - K72405EU, K72421/2/3/4WW

USB-Port-Schlösser

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

K67913WW | K67914WW | K67915WW

VeriMark™ und VeriMark™ Pro Fingerabdrucktasten

Mit der Zunahme umfangreicher Datenschutzverletzungen und dem wachsenden Bewusstsein steigt auch der Wunsch nach einer einfachen, sicheren und zuverlässigen Möglichkeit, persönliche und betriebliche Daten zu schützen – einer Möglichkeit, die am besten auch mit Unternehmenssoftware wie Windows Hello™ und Windows Hello™ for Business, Google G Suite, Azure, Active Directory, Dropbox, Github und Ähnlichen kompatibel ist.

	VeriMark™	VeriMark™ Pro
Fingerabdrucksensor	Synaptics FS4300 Biometrische Daten in Host-PC/ Software gespeichert	Synaptics FS7600 Biometrische Daten in Fingerabdrucktaste/Hardware gespeichert
FIDO Standard / Sicherheitsstufe	FIDO U2F AES-256 / SHA-256	FIDO2 U2F-kompatibel AES-256 / SHA-256, TSL1.2
Falschrückweisungsrate	3 %	2 %
Falschakzeptanzrate	0,002 %	0,001 %
Betriebssystem	Windows 10, 8.1, 7	Windows 10, 8.1, 7
Windows Hello	Windows Hello™	Windows Hello for Business™
Artikelnummer	**K67977WW**	**K64704WW**

Fazit

Obwohl die DSGVO ein EU-Gesetz ist, hat sie weltweite Bedeutung. Jede Organisation, die personenbezogene Daten über Personen in der EU besitzt oder verarbeitet, unterliegt der DSGVO und muss bei Verstößen mit empfindlichen Strafen rechnen. Der enorme Anstieg an Datenschutzverletzungen in der ganzen Welt wird oft mit dem Internet und Malware-Angriffen erklärt, aber auch die mangelhafte physische Sicherheit der IT-Hardware bleibt eine bedeutende Fehlerquelle.

Die Kooperationsbereitschaft der Mitarbeiter ist ein wesentlicher Bestandteil zur Einhaltung der DSVGO-Richtlinien. Die Überwindung von Gewohnheiten und Einschränkungen kann hier einen wichtigen Beitrag leisten. Blickschutzfilter verhindern unbefugte Einblicke in Daten auf dem Bildschirm, und Laptop- und Geräteschlösser können Diebe abschrecken sowie Diebstähle verhindern. Kensington bietet benutzerfreundliche Online-Produktfinder,

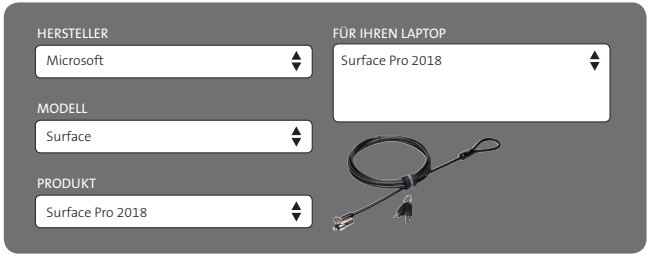
mit denen Sie den richtigen Blickschutzfilter und das richtige Schloss für Ihre Geräte finden, ganz gleich welche Marken und Modelle. Dazu gibt es zahlreiche weitere Produkte, mit denen Sie Ihre Geräte sowohl im Büro als auch unterwegs effektiv schützen können.

Finden Sie das richtige Kensington Produkt ...

Laptop- oder Geräteschloss

www.kensington.com/securityselector

Wählen Sie Marke, Modell und Produktnummer oder gehen Sie direkt zum Gerät, um das dafür empfohlene Schloss zu finden.



Blickschutzfilter

www.kensington.com/privacy-selector

Grenzen Sie Ihre Suche ein, indem Sie Geräteart bzw. Bildschirmgröße auswählen oder ganz einfach die Modellnummer eingeben.

* Sicherheitsschlösser und Blickschutzfilter unterstützen die DSGVO-Konformität

Kensington The Professionals' Choice™

Kensington®

Kensington bietet preisgekrönte Lösungen für Unternehmen, die ihren Mitarbeitern die richtigen Mittel für Spitzenleistung und Erfolg bereitstellen möchten. Kensington genießt seit über 35 Jahren das Vertrauen von Unternehmen. Die Akzeptanz und der Erfolg der Marke beruht auf ihrer Entschlossenheit, die Anforderungen der sich ständig ändernden Arbeitswelt von heute vorherzusehen und zu erfüllen.

Kensington verfolgt diesen zukunftsorientierten Ansatz, gepaart mit den drei stetigen Grundwerten:

Qualität

Dank mehr als 35 Jahren Erfahrung in der Fertigung von IT-Hardware-Produkten in großen Stückzahlen verfügt Kensington über eine strikte Qualitätskontrolle, die bedeutet, dass alle Produkte über den Branchenstandard hinaus getestet werden.

Support

Kensington hat Kunden in aller Welt, ob große oder kleine Unternehmen. Jeder Kunde wird ausnahmslos als professioneller Nutzer mit professionellen Ansprüchen behandelt.

Design

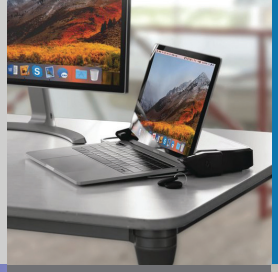
Die preisgekrönten Lösungen von Kensington sind das Ergebnis sorgfältiger Forschung, Planung und Entwicklung.. So erfüllen sie die sich ständig ändernden Leistungs- und Kompatibilitätsanforderungen anspruchsvoller professioneller Nutzer.

Quellen

1. Kensington Umfrage zu IT-Sicherheit und Laptop-Diebstahl, August 2016
2. Google hit with £44m GDPR fine over ads - bbc.co.uk/news/technology-46944696
3. 2018 Data Breaches - Privacy Rights Clearinghouse
4. Breach Level Index, März 2019
5. Kensington Umfrage zu IT-Sicherheit und Laptop-Diebstahl, August 2016
6. Information Commisioner's Office - ico.org.uk/action-weve-taken/data-security-incident-trends
7. Computer with data on 20,000 people stolen in Denmark - thelocal.dk/20181211/computer-with-data-on-20000-people-stolen-in-denmark
8. 37,000 Eir customers face data breach in laptop theft - independent.ie/business/technology/37000-eir-customers-face-data-breach-in-laptop-theft-37240098.html
9. Financial Services Breach Report, Bitglass, 2016
10. Verizon Data Breach Investigations Report 2016
11. IDC Executive Brief 2010: Laptop Theft: The Internal and External Threat
12. Ponemon Institute: Visual Hacking Experiment, 2016
13. IDC White Paper 2007: The Threat of Theft and Loss of Laptops for the SME

Kensington®

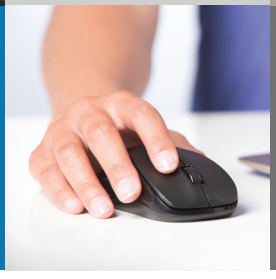
Sicherheit



Schlösser und Docking Stations

Konnektivität

Steuerung



Taschen und Hüllen

Ergonomie

Kensington

The Professionals' Choice™