KEEPING YOUR DATA SAFE AND SECURE

Encryption - why is it important?

With the massive increase in the use of mobile devices, and attacks against government networks and business databases escalating, data security and encryption continues to be a hot topic. Encryption scrambles data in such a way that only someone with the correct code or key can read it, so if your HDD is lost or stolen, you can be confident that the content of the drive cannot be accessed.

Furthermore, with the introduction of GDPR in Europe three years ago (and the UK equivalent UK-GDPR after Brexit) and the huge fines that can be imposed, it is vital for businesses to ensure that their critical and sensitive information is protected properly. One way companies are advised to process personal data securely is by having an encryption policy incorporating encryption solutions.

Read on to find out more about the GDPR fines imposed in the last 12 months and how Verbatim could help customers keep their data stored safely and securely.

GDPR fines of 2020 and 2021 (so far...)

Penalties imposed following serious GDPR breaches according to research from DLA Piper, between January 26, 2020, and January 27, 2021*

GDPR fines rose by nearly 40%

Penalties under GDPR totaled €158.5 million ($191.5 million)

121,165 data breach notifications (19% more than the previous 12 month period)

We've summarised below the biggest GDPR fines of 2020 and 2021*:

Company	Fines (€)($)
Google	50 M€ (56.6 M$)
H&M	35 M€ (41 M$)
TIM	27.8 M€ (31.5 M$)
British Airways	22 M€ (26 M$)
Marriot	20.4 M€ (23.8 M$)

Company	Fines (€)($)
Wind	17 M€ (20 M$)
Notebooksbilliger.de	10.4 M€ (12.5 M$)
Google	7.0 M€ (7.9 M$)
Caixabank	6.0 M€ (7.2 M$)
BBVA (bank)	5.0 M€ ($6.0 M$)

Source*: https://www.tessian.com/blog/biggest-gdpr-fines-2020/

Data Protection and Security

So, why do these breaches and violations happen? Well, the GDPR has seven protection and accountability principles which companies must follow when processing customer data**:

1. **Lawfulness, fairness and transparency** – Processing must be lawful, fair, and transparent to the data subject.
2. **Purpose limitation** – You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. **Data minimization** – You should collect and process only as much data as absolutely necessary for the purposes specified.
4. **Accuracy** – You must keep personal data accurate and up to date.
5. **Storage limitation** – You may only store personally identifying data for as long as necessary for the specified purpose.
6. **Integrity and confidentiality** – Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7. **Accountability** – The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

If the above principles are not followed and violated against, companies have to face hefty fines.

At Verbatim, we are committed to helping customers keep their data safe – and supporting businesses with encrypted products to adhere with GDPR and UK-GDPR. We offer a wide range of portable storage devices that are protected by the AES 256-bit encryption system which has never been cracked.

Our devices, be they HDDs, SSDs, USB drives or HDD enclosures are protected by keypads, fingerprint recognisers or conventional computer password entry. As long as the passwords (or fingers) cannot be accessed by the wrong people, the stored data is secure.

Keep your data safe and secure with Verbatim! Take a look at our encrypted range.

Source**: https://gdpr.eu/what-is-gdpr/

Encrypted Storage: Hard Drive & SSD solutions

Our large capacity hard drives or fast performing SSDs deliver 256-bit AES hardware encryption to protect your crucial data on the move. They're ideal for your important work documents, personal files or even family memories that you want to keep safe.

Secure Portable Hard Drive with Keypad Access

- Premium AES 256-bit hardware encryption
- Built-in keypad for passcode input (5 to 12 digits)
- Can be used with TVs (feature not possible with regular encrypted HDDs)
- USB 3.2 GEN 1 with USB-C™ connection plus USB-C™ adapter
- LED power / encryption status indicators
- Nero Backup Software included

PART NO	DESCRIPTION
53401	Store 'n' Go Keypad Secure Portable HDD 1 TB
53403	Store 'n' Go Keypad Secure Portable HDD 2 TB

USB-C™

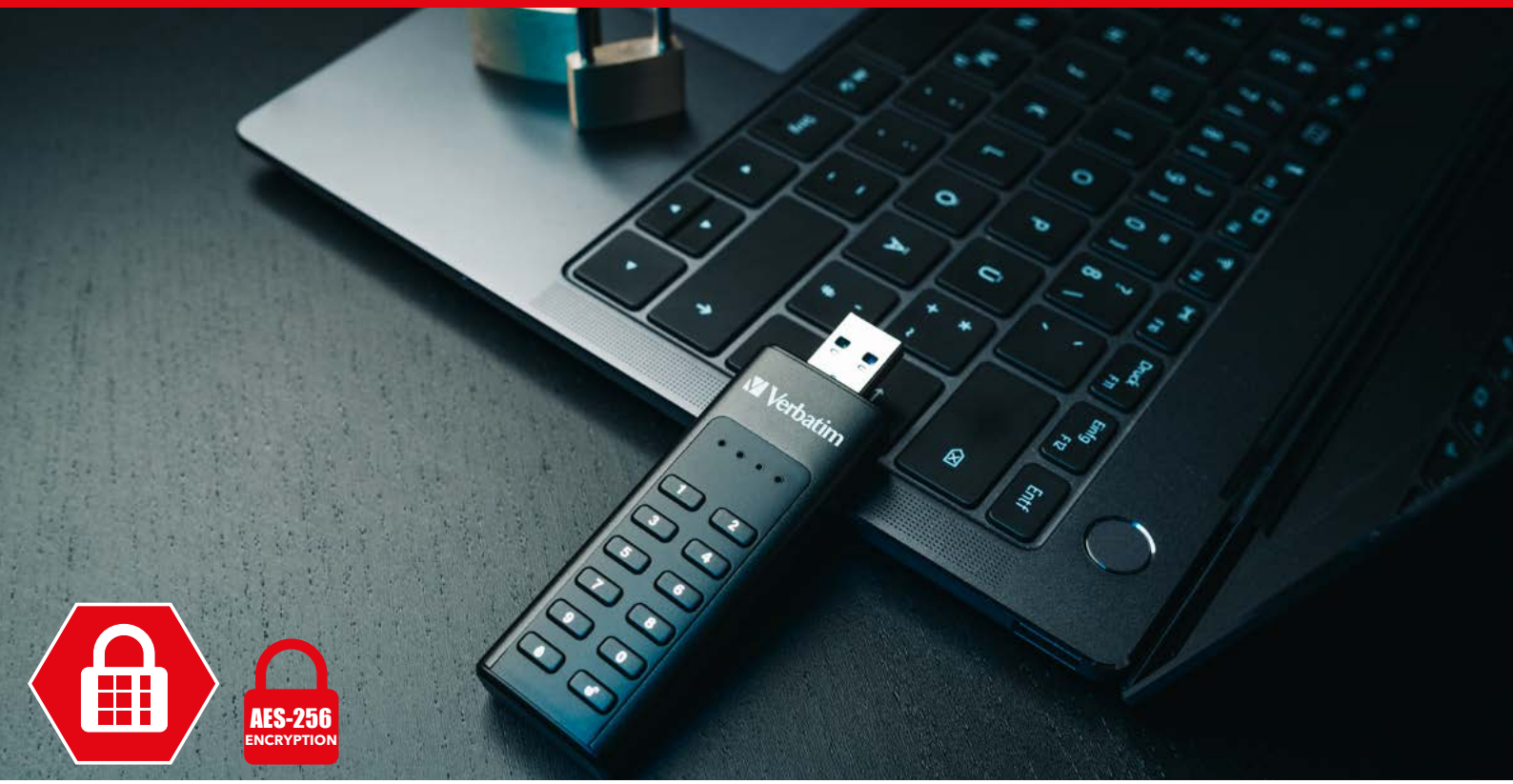
Store 'n' Go Secure Portable SSD with Keypad Access

- Premium AES 256-bit Hardware Encryption
- Built-in keypad with passcode input (5 to 12 digits)
- SSDs use flash memory storage for faster speeds, higher performance and greater reliability
- USB 3.2 GEN 1 with USB-C™ connection
- LED power / encryption status indicators
- More secure than software encryption
- Nero Backup Software

PART NO	DESCRIPTION
53402	Store 'n' Go Keypad Secure Portable SSD 256 GB

USB-C™

Encrypted Storage: USB Solutions



Keypad Secure USB Drive delivers premium 256-bit AES hardware security encryption and integrated password protection, keeping your confidential data protected. If you are looking for something secure but affordable at the same time, then look no further then the Secure Data Pro Encrypted USB.

Keypad Secure USB Drive

- AES 256-bit Hardware Encryption, seamlessly encrypts all data on the drive in real-time
- Built-in keypad for passcode input (up to 12 digits)
- Can be used with TVs (feature not possible with regular encrypted devices)
- LED power / encryption status indicators
- Does not store password in the computer or the system's volatile memory, therefore far more secure than software encryption
- PC and Mac compatible
- Available with either USB 3.2 Gen 1 or USB 3.2 GEN 1 with USB-C™ connection

PART NO	DESCRIPTION
Keypad Secure USB 3.2 Gen 1	
49427	Keypad Secure USB 3.2 Gen 1 Drive 32GB
49428	Keypad Secure USB 3.2 Gen 1 Drive 64GB
49429	Keypad Secure USB 3.2 Gen 1 Drive 128GB
Keypad Secure USB-C™	
49430	Keypad Secure USB-C™ Drive 32GB
49431	Keypad Secure USB-C™ Drive 64GB
49432	Keypad Secure USB-C™ Drive 128GB

USB-C™

Click here to watch video

Secure Data Pro
Encrypted USB 3.2 Gen 1 Drive

- Hardware-based 256-bit AES encryption with Security controller based hardware
- Password protection application
- Password hashing algorithm
- Hack resistant password entry

PART NO	DESCRIPTION
98664	Secure Data Pro USB Drive USB 3.2 Gen 1 16GB
98665	Secure Data Pro USB Drive USB 3.2 Gen 1 32GB
98666	Secure Data Pro USB Drive USB 3.2 Gen 1 64GB

Encrypted Storage: Fingerprint Solutions

Commuting again for work? Being able to save your work safely and securely is one thing you need to guarantee. Verbatim's award winning encrypted fingerprint solutions will give you peace of mind that your data is saved securely, wherever you are!

Fingerprint Secure Hard Drive

- Access using fingerprint recognition
- USB-C™ connection
- Premium 256-bit AES hardware encryption
- Up to eight authorised users plus one administrator (via password)
- Store and carry confidential data while being protected from loss or hacking
- Stylish black design with a 3D surface matching the SSD range
- USB 3.2 GEN 1 with USB-C™ connection plus USB-C™ adapter
- LED power / encryption status indicators
- Nero Backup Software included

PART NO	DESCRIPTION
53650	Fingerprint Secure Portable HDD 1 TB
53651	Fingerprint Secure Portable HDD 2 TB

Fingerprint Secure USB Drive

- Sleek aluminium USB 3.2 Gen 1 drive with integrated fingerprint scanner
- Access using fingerprint from authorised user
- Premium 256-bit AES hardware security encryption
- Up to five authorised users plus one administrator
- Store and carry confidential data while being protected from loss or hacking

PART NO	DESCRIPTION
49337	Fingerprint Secure USB 3.2 Gen 1 Drive 32GB
49338	Fingerprint Secure USB 3.2 Gen 1 Drive 64GB
49339	Fingerprint Secure USB 3.2 Gen 1 Drive 128GB