ARE YOU GDPR COMPLIANT?

YOUR PRIVACY IS IMPORTANT

Keeping your data safe and secure while on the move is a prime concern – not only for businesses, but also from a personal perspective.

What if an employee takes customer data home with them on a hard drive and loses it or has it stolen? Or if you mislay a USB drive that contains files detailing your banking records?

Globally, more than 2 million of these small storage devices are lost each year and studies have shown that over half of dropped USB sticks get plugged in.

One easy step to reduce this risk is to use encrypted devices, which scrambles the data in such a way that only someone with the correct code or key can read it.

Can you afford **not** to encrypt your data?

Verbatim™

Technology you can trust

DID YOU KNOW?

14,717,618,286

DATA RECORDS HAVE BEEN LOST OR STOLEN SINCE 2013

In only **4%** of these cases the stolen data was **encrypted** rendering it useless to the thieves.

Out of the total number of records stolen, the **social media** sector saw the biggest increase in security incidents, rising from 1.51% in 2017 to **56.18%** in 2018. In the same timeframe, the number of breaches in the healthcare sector showed a significant decline. In the first half of 2018 the government, education, entertainment, financial services and non-profit sectors reported **50-100% fewer security breaches** than the previous year.

Source: Breach level index 17/04/19

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

Every day	Every hour	Every minute	Every second
6,404,534	266,856	4,448	74

WHAT IS GDPR?

GDPR - GENERAL DATA PROTECTION REGULATION

The enforcement of GDPR has made data protection law identical throughout the single European market.

It has given businesses a simpler and clearer legal environment in which to operate and people more say in what companies can do with their data.

There are also tougher fines for companies that do not comply. Organizations can be fined up to 4% of annual global turnover or €20 Million.

All of this makes it more important than ever to ensure that your critical and sensitive information is protected properly.

MALWARE EXPLAINED

Viruses: By attaching themselves to files and infecting other files, they can spread uncontrollably, damaging a system's core functionality and deleting or corrupting files.

Rootkits: Software that allows an intruder to obtain root access to a computer system. It is often hidden and can go unnoticed by antivirus detection and removal.

Spyware: A program that hides in the background and spies on users, taking notes on their online activity, including passwords, credit card numbers, surfing habits and more.

Trojans: Disguised as legitimate software, users download trojans thinking they are useful pieces of software, instead they end up with an infected computer.

Worms: These are self-replicating programs intended to spread malicious code. Using network interfaces, they can infect entire networks, either local or across the Internet.

Ransomware is a type of malware with the ability to silently encrypt your files and make your system unusable, before demanding an online ransom payment in exchange for a decrypt key.

AES 256-BIT ENCRYPTION

WHAT IS AES 256-BIT ENCRYPTION?

AES stands for Advanced Encryption Standard. It is a symmetric block cypher that is adopted throughout the world to encrypt sensitive data.

256-bit refers to the length of the encryption key used to encrypt a data stream or file. a hacker or cracker will require 2^{256}* different combinations to break a 256-bit encrypted message.

AES has never been cracked and is safe against any brute force attacks.

*2^{256} =115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936

FINGERPRINT ACCESS STORAGE DEVICES

Uses your unique biometric data for complete information security

FINGERPRINT SECURE HARD DRIVE

- USB-C™ portable hard drive with integrated fingerpint scanner
- Access using fingerprint from authorised user
- AES 256-bit hardware security encryption
- Up to eight authorised fingerprint users and one administrator (via password)
- Store and carry confidential data while being protected from loss or hacking
- USB-C™ to USB-A cable and USB-C™ adapter
- Nero Backup Software included

53650 1TB | 53651 2TB

FINGERPRINT SECURE USB DRIVE

- Sleek aluminium USB 3.0 drive with integrated fingerpint scanner
- Access using fingerprint from authorised user
- AES 256-bit hardware security encryption
- Up to five authorised users and one administrator
- Store and carry confidential data while being protected from loss or hacking

49337 32GB | 49338 64GB | 49339 128GB

SECURE PRO USB DRIVE

ENCRYPTED USB

- Mandatory 100% drive encryption
- Up to 12-digit passcode
- 256-bit AES encryption with security controller based hardware
- Preloaded with an intuitive autorun security application
- Password hashing algorithm
- Hack resistant password entry - erases data after 10 failed attempts
- No admin rights required on host PC
- PC and Mac compatible

98664 16GB | 98665 32GB | 98666 64GB

PINCODE ACCESS STORAGE DEVICES

Requires your individual passcode to be entered to get access to any data

SECURE PORTABLE HDD WITH KEYPAD ACCESS

- Mandatory 100% 256-bit AES hardware encryption
- 5 to 12-digit passcode
- NERO backup software
- Mac and PC compatible
- Type-C, USB 3.1 Gen 1
- Hack resistant password entry - erases data after 20 failed attempts

53401 1TB | 53403 2TB

SECURE PORTABLE SSD WITH KEYPAD ACCESS

- SSDs use flash memory storage for faster speeds, higher performance and greater reliability
- Mandatory 100% 256-bit AES hardware encryption
- 5 to 12-digit passcode
- NERO backup software
- Mac and PC compatible
- Type-C, USB 3.1 Gen 1
- Hack resistant password entry - erases data after 20 failed attempts

53402 256GB

SECURE PORTABLE USB DRIVE WITH KEYPAD ACCESS

- 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
- PC and Mac compatible
- Available with either USB 3.0 or USB 3.1 GEN 1 with USB-C™ connection

USB 3.0: 49427 32GB | 49428 64GB | 49429 128GB **USB-C™:** 49430 32GB | 49431 64GB | 49432 128GB

SECURE DESKTOP HDD ENCLOSURE KIT WITH KEYPAD ACCESS

- Built-in keypad for secure password input
- AES 256-bit hardware encryption
- 3.5” hard drive enclosure
- Fits any standard 3.5” internal SATA hard drive
- Easy installation. No advanced technical knowledge required
- USB-C™ to USB-A connection

53405

BACKUP AND ARCHIVING

Regular back-ups protect against both accidental or malicious data loss - anything from hardware faults and viruses to human error or theft - as they can be used to restore original data files.

Choosing the right media and back-up procedure depends on many elements:

- The amount of data being saved
- The perceived value of the data
- The levels of accepted risk
- The length of time you need to keep the data for

BEST PRACTICE - APPLY THE 3-2-1 BACK UP RULE

3

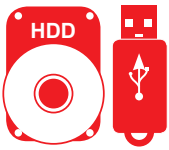
HAVE AT LEAST THREE COPIES OF YOUR DATA

In addition to your primary data, you should also have at least two more backups, which will help significantly reduce the risk of losing data. These could be physical and / or cloud solutions.

2

STORE THE COPIES ON AT LEAST TWO DIFFERENT MEDIA

It is best practice to keep copies of your data on at least two different storage types, such as internal hard disk drives AND removable storage media (tapes, external hard drives, USB drives, SD-cards, CDs, DVDs.)

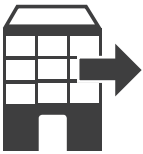


1

KEEP AT LEAST ONE OFFSITE BACKUP COPY

It’s obvious really, but it’s not a good idea to keep your external storage device in the same room as your production storage.

If there is a fire, flood or burglary - you would lose all of your data.



BEST PROTECTION
AGAINST ATTACK
ARCHIVE YOUR DATA

To be completely protected, a user or organisation needs to have data backed up and archived offline.

Any device that is attached to an attacked system or network is vulnerable.

If your back up HDD is plugged into your laptop when a piece of ransomware software is installed it will also be encrypted. Having your most important data archived to optical media can eliminate this risk.

OPTICAL MEDIA & DRIVES FOR ARCHIVING

- Blu-ray, DVD, CD media - the best solution for long term storage (25 - 100 years)
- Use with Verbatim's external DVD and Blu-ray Writers
- Nero Burn&Archive software free with Verbatim DVD and Blu-ray Writers

43888 | 43889 | 43890 | 98938 | 43894

RFID SECURE BAGS

SECURE BAGS
WITH RFID SECURE POCKET

- Range includes rollers, backpacks, camera bags, notebook cases, messenger bags
- Includes special RFID secure pocket to prevent credit card scanning

Paris 49852 | London 49855

ARE YOU GDPR COMPLIANT?

Verbatim Head Office

Verbatim GmbH
Düsseldorfer Str. 13,
D - 65760 Eschborn,
Germany
T: +49 (0) 6196 900 10
E: info.germany@verbatim-europe.com

Verbatim™
Technology you can trust

www.verbatim-europe.com/security