



## MANTIENI I TUOI DATI AL SICURO E PROTETTI

### Crittografia: è davvero così importante?

Con il massiccio aumento dell'uso di dispositivi mobili e l'escalation degli attacchi contro le reti governative e i database aziendali, la sicurezza dei dati e la crittografia continuano a essere un tema caldo. La crittografia codifica i dati in modo tale che solo chi ne possiede il codice corretto può leggerli, quindi se il tuo HDD venisse perso o rubato, puoi essere certo che il contenuto dell'unità non sarà accessibile.

Inoltre, con l'introduzione del GDPR in Europa tre anni fa e le enormi sanzioni che possono essere imposte, è fondamentale per le aziende garantire che le loro informazioni critiche e sensibili siano protette adeguatamente. Un modo in cui si consiglia alle aziende di elaborare i dati personali in modo sicuro è disporre di una politica di crittografia che incorpori soluzioni di crittografia.

Continua a leggere per saperne di più sulle sanzioni previste dal GDPR negli ultimi 12 mesi e su come Verbatim può aiutare a conservare i propri dati in modo sicuro e protetto.

# GDPR: sanzioni 2020 - 2021 (fino ad oggi...)



Sanzioni imposte a seguito di gravi violazioni del GDPR secondo una ricerca di DLA Piper, tra il 26 gennaio 2020 e il 27 gennaio 2021 \*

Le sanzioni previste dal GDPR sono aumentate di quasi il 40%



Le sanzioni ai sensi del GDPR ammontavano a 158,5 M€ (191,5 M\$)



121.165 notifiche di violazione dei dati (+19% rispetto ai 12 mesi precedenti)



Di seguito le multe più elevate del GDPR del 2020 e del 2021 \*:

Società	Sanzione (€/€)
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\$)

Società	Sanzione (€/€)
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\$)

# Protezione e sicurezza dei dati



Perché si verificano queste violazioni e violazioni? Ebbene, il GDPR ha sette principi di protezione e responsabilità che le aziende devono seguire durante l'elaborazione dei dati dei clienti \*\*:

1. **Liceità, correttezza e trasparenza:** il trattamento deve essere lecito, equo e trasparente nei confronti dell'interessato.
2. **Limitazione dello scopo:** è necessario elaborare i dati per gli scopi legittimi specificati esplicitamente all'interessato al momento della raccolta.
3. **Minimizzazione dei dati:** raccogliere ed elaborare solo la quantità di dati assolutamente necessaria per gli scopi specificati.
4. **Precisione:** è necessario mantenere i dati personali accurati e aggiornati.
5. **Limitazione dell'archiviazione:** è possibile archiviare i dati di identificazione personale solo per il tempo necessario per lo scopo specificato.
6. **Integrità e riservatezza:** l'elaborazione deve essere eseguita in modo tale da garantire sicurezza, integrità e riservatezza appropriate (**ad esempio utilizzando la crittografia**).
7. **Responsabilità:** il titolare del trattamento dei dati è responsabile di essere in grado di dimostrare la conformità al GDPR con tutti questi principi.

Se questi principi non vengono seguiti ma addirittura violati, le aziende sono soggette a multe salate. In Verbatim, ci impegniamo ad aiutare i clienti a mantenere i propri dati al sicuro e a supportare le aziende con supporti con crittografia nel rispetto del GDPR. Offriamo una vasta gamma di dispositivi di archiviazione portatili protetti dal sistema di crittografia AES a 256 bit che non è mai stato violato.

I nostri dispositivi, siano essi HDD, SSD, chiavette USB o custodie per HDD sono protetti da tastierino, lettori di impronte digitali o password da digitare nel computer. Finché le password (o le dita) non possono essere accessibili dalle persone sbagliate, i tuoi dati sono al sicuro.

**Mantieni i tuoi dati al sicuro e protetti con Verbatim! Scopri la nostra gamma di prodotti di archiviazione con crittografia dei dati.**

# Archiviazione con crittografia: Hard Drive & SSD



I nostri dischi rigidi di grande capacità o SSD ad alte prestazioni utilizzano la crittografia hardware AES a 256 bit per proteggere i tuoi dati più importanti in qualsiasi momento. Sono ideali per i tuoi documenti di lavoro importanti, file personali o anche ricordi di famiglia che desideri tenere al sicuro.

## Secure Portable HDD con codice di accesso

- Crittografia Hardware a 256 bit AES
- Tastierino integrato per inserimento del codice
- Utilizzabile con i televisori (funzionalità non possibile con i normali dischi fissi crittografati)
- USB 3.1 Gen 1 con connessione USB-C™
- Indicatore LED alimentazione / stato di codifica
- Software Nero Backup incluso

## Secure Portable SSD con codice di accesso

- Crittografia Hardware a 256 bit AES
- Tastierino integrato per inserimento del codice
- Le memorie SSD utilizzano spazio di archiviazione con memoria flash per la massima rapidità, performance migliori e maggior affidabilità
- USB 3.1 Gen 1 con connessione USB-C™
- Indicatore LED alimentazione / stato di codifica
- Software Nero Backup incluso

CODICE	DESCRIZIONE
--------	-------------

53401	Store 'n' Go Keypad Secure Portable HDD 1 TB
-------	--

53403	Store 'n' Go Keypad Secure Portable HDD 2 TB
-------	--



USB-C™

CODICE	DESCRIZIONE
--------	-------------

53402	Store 'n' Go Keypad Secure Portable SSD 256 GB
-------	--



USB-C™



# Archiviazione con crittografia: memorie USB



Keypad Secure USB Drive offre crittografia di sicurezza hardware AES a 256 bit premium e protezione con password integrata, mantenendo protetti i tuoi dati riservati. Se stai cercando qualcosa di sicuro ma allo stesso tempo conveniente, non cercare oltre, scegli Secure Data Pro Encrypted USB.

## Keypad Secure USB Drive

- Crittografia Hardware a 256 bit AES, cripta costantemente tutti i dati sull'unità in tempo reale
- Tastierino integrato per inserimento della password (fino a 12 cifre)
- Utilizzabile con i televisori (funzionalità non possibile con i normali dispositivi crittografati)
- Connessione USB 3.2 Gen 1
- Indicatori alimentazione LED / stato criptato
- Non conserva la password nel computer o nella memoria volatile del sistema, garantendo quindi una maggiore protezione rispetto alla crittografia software
- Compatibile con PC e Mac
- Enclosure in alluminio/plastica

### CODICE DESCRIZIONE

#### 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



Clicca QUI  
per il video



## Secure Data Pro

### Encrypted USB 3.2 Gen 1 Drive

- Crittografia hardware AES a 256 bit basata su Security controller
- Applicazione di protezione con password
- Algoritmo di hash della password
- Immissione della password resistente agli hack

### CODICE DESCRIZIONE

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



# Archiviazione con crittografia e impronte digitali



Di nuovo avanti e in dietro per lavoro? Essere in grado di salvare il tuo lavoro in modo sicuro e protetto è una cosa che devi garantire. Le pluripremiate soluzioni di impronte digitali crittografate di Verbatim ti daranno la tranquillità che i tuoi dati vengano salvati in modo sicuro, ovunque tu sia!

## Fingerprint Secure Hard Drive

- Accesso tramite riconoscimento dell'impronta digitale
- Connessione USB-C™
- Crittografia Hardware AES a 256 bit
- Fino a 8 utenti e un amministratore (via password)
- Archivia e trasporta dati riservati mentre sei protetto da perdita o hacking
- Elegante design nero con una superficie 3D che si abbina alla gamma SSD
- USB 3.2 GEN 1 con connessione USB-C™ e adattatore USB-A / USB-C™
- Indicatori alimentazione LED / stato criptato
- Software Nero Backup incluso

CODICE	DESCRIZIONE
53650	Fingerprint Secure Portable HDD 1 TB
53651	Fingerprint Secure Portable HDD 2 TB



## Fingerprint Secure USB Drive



- Chiavetta USB 3.2 Gen 1 elegante in alluminio con scanner integrato per le impronte digitali
- Accesso mediante impronta digitale
- Crittografia di sicurezza hardware AES a 256 bit
- Fino a sei utenti autorizzati, compreso un amministratore (tramite password)
- Conservazione e trasporto di dati riservati protetti da eventuali smarrimenti o hacking

CODICE	DESCRIZIONE
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