

# Privacy by Design

Learn how **Common Criteria** certified hard drives aid in **GDPR** compliance.



# Data Encryption Goes Global

## Common Criteria Is Now an International Standard

Following a rigorous evaluation by independent industry authorities, Seagate® has achieved Common Criteria accreditation for select products in our Nytro®, Exos™, and BarraCuda® portfolios—meaning they meet internationally-recognized regulations across 28 member nations and are **certified for classified environments** within those countries.

### What Is Common Criteria?

- It's an international standard for assessing the security functionality of information assurance (IA) and IA-enabled technology products.
- It's required for technology used in US and EU government markets.
- It assures buyers that a product's design, specs, and implementation have been evaluated in a thorough, standardized manner.
- It benefits non-government markets like finance, critical infrastructure, and health care.

[Learn more about Common Criteria](#)

Learn more about Seagate Common Criteria certified products [at NIAP](#)  
Seagate Validation ID: 10857



## How We'll Help You with GDPR Compliance

By deploying Seagate Common Criteria certified hard drives, you're using a valuable tool to help meet some of the key requirements of Privacy by Design—an important component of GDPR.

### What Is GDPR?

- It helps protect the data privacy of EU citizens by reshaping the way organizations approach data privacy. Aside from the EU, its' setting the standard for how other countries approach data protection laws and regulations.
- Organizations found to be non-compliant face penalties.
- Effective May 25, 2018, it applies to organizations inside or outside the EU that offer goods or services to, or process private data of, EU citizens.
- **Privacy by design** seeks to build data protection into processes, systems, and hardware that manage personally identifiable information. Encrypting data at rest is part of that.

## GDPR Requirement

### Security of Processing (Article 32)

Encryption can be an appropriate technical measure.

We engineer encrypted drives that suit a wide array of applications.

### Data Protection by Design & by Default (Article 25)

Controllers must implement technical and organizational measures for data protection.

We keep a secure supply chain through each drive's lifecycle.

### Accuracy, Confidentiality & Integrity (Article 5)

Data needs to be protected against unlawful processing, loss, and exposure.

We offer self-encrypting drives (SEDs) and FIPS-approved drives.

### Right to Erasure (Article 17)

When appropriate, an individual's personal data must be erased within one month of request.

We've built an Instant Secure Erase feature so you can easily change data access.

## Seagate Solution

[Learn more about GDPR](#)

## 3 Tips for Protecting Your Data

1. Use Secure Encrypted Drives (SEDs) to encrypt user data and lock data during transport.
2. Utilize AES 256 encryption (ISO/IEC 18033-3) and hard drives that are Common Criteria certified. (ISO/IEC 15408).
3. Practice end-of-life data erasure on devices.

Seagate Secure devices offer two service levels, **Essential** and **Certified**.

Essential features are standard for all, while Certified assists industries such as government, healthcare, finance, and education.



	ESSENTIAL	CERTIFIED
Self-Encrypting Drive	<input type="radio"/>	<input checked="" type="radio"/>
Secure Download and Diagnostics	<input type="radio"/>	<input checked="" type="radio"/>
Instant Secure Erase	<input type="radio"/>	<input checked="" type="radio"/>
Secure Supply Chain	<input type="radio"/>	<input checked="" type="radio"/>
Secure Boot	<input type="radio"/>	<input checked="" type="radio"/>
FIPS 140-2		<input checked="" type="radio"/>
Common Criteria		<input checked="" type="radio"/>
Trade Agreement		<input checked="" type="radio"/>

## Learn about Seagate Secure Products and Purchasing

Contact a Seagate representative or visit:

[seagate.com/enterprise-storage/enterprise-security/](https://www.seagate.com/enterprise-storage/enterprise-security/)

Look for drives that are FIPS 140-2 approved, Common Criteria certified, and tamper evident.