GDPR

STRONGKEY™

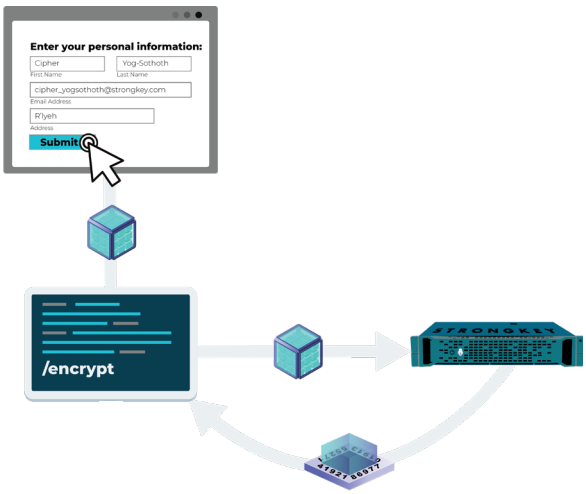
WHAT YOU NEED TO KNOW TO PROTECT YOUR DATA FIRST.

For almost two decades, we've been creating and implementing data protection solutions that **far exceed some of the most difficult compliance requirements.** We are excited to help lead the way into a new era of digital trust, and we're here to help your organization with GDPR compliance. Let's take a look at four of the most difficult requirements of GDPR, as well as how StrongKey technology can help.

Pseudonymization

This difficult-to-pronounce word is a synonym of a widely used technology in the payment processing industry: tokenization—a method of replacing real data with an encrypted "token" or representation of that data so it is unidentifiable. StrongKey has been securing cardholder data and payment information for over a decade using tokenization and encryption services backed by one of the most secure technologies: public key cryptography.

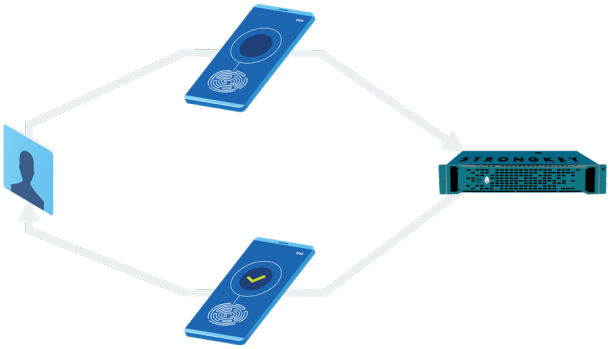
StrongKey's tokenization offering is one of the strongest means to meet GDPR's pseudonymization requirement.



Unambiguous Consent

GDPR requires explicit consent from a user to allow their data to be processed and stored. However, to be sure the consent is legitimate, the user identity must be verifiable. Using FIDO2 strong authentication, a user is verified through public key cryptography without the use of a password, ensuring that the user is, in fact, who they say they are—making the consent legitimate and unambiguous.

StrongKey's open source FIDO2 Server and our authentication expertise can you create not just a compliant environment, but also a more convenient, password-free one.



Data Integrity Verification

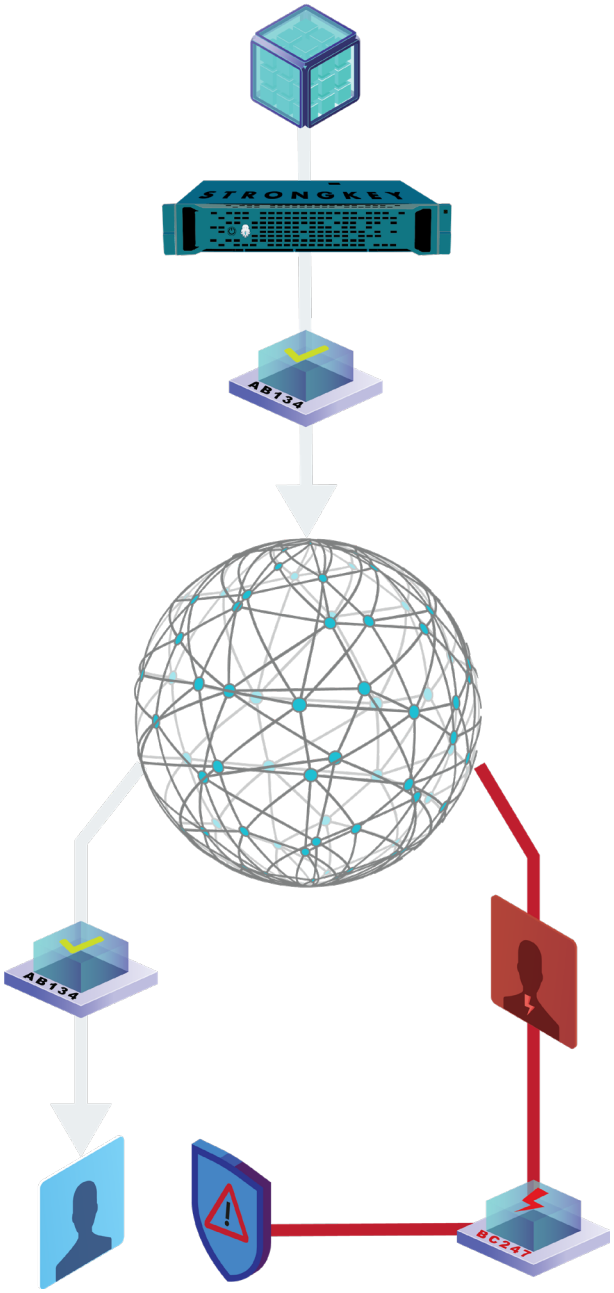
GDPR mandates protection against the alteration of data (maintaining data integrity). Data integrity means the accuracy of the data remains over its life. This protects against accidental changes like human error or intentional attacks designed to alter the data. One of the best ways to protect against alteration of data is to ensure its validity through digital signatures.

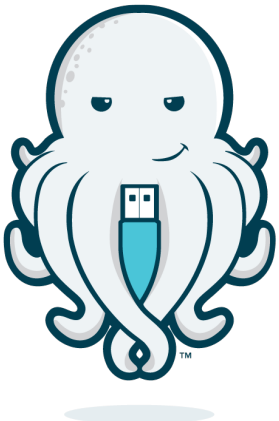
StrongKey easily integrates digital signature capability into our customers' transactions, applications, and documents. Working in concert with our encryption and tokenization, this is an extremely strong way to meet GDPR mandates for data integrity.

Data Protection by Design

One of the most compelling tenets and memorable lines of GDPR is in Article 25: "Data protection by design and by default." This expressly mandates that technical and organizational measures be taken to ensure that: (1) data protection principles are designed into the system; (2) only necessary data is processed for each purpose; and (3) an approved certification method is used to demonstrate compliance.

Through our product architecture and accessible documentation, StrongKey can help an organization comply with this mandate both by design and by default.





ABOUT STRONGKEY

StrongKey makes data breaches irrelevant by redefining how businesses and government agencies secure their information against the inevitability of a breach. While other security companies focus on protecting the perimeter, StrongKey secures the core through strong authentication, encryption, digital signatures and hardware-backed key management—keeping the core safe even with an attacker on the network. Based in Silicon Valley, CA and Durham, NC, StrongKey has provided cryptographic security solutions for over 18 years and is trusted in mission-critical business operations by some of the largest companies in payment processing, e-commerce, healthcare, and finance. Learn more at www.strongkey.com.

strongkey.com | getsecure@strongkey.com | 408.331.2000