STRONGKEY

Complying with GDPR – Data Protection Done Right.

INTRODUCTION

The introduction of the General Data Protection Regulation (GDPR) has done much to protect the fundamental rights of consumers, but has also introduced complexity for organizations to comply. This legislation names a host of requirements, including many related to data policy, assessing your usage of sensitive data, and understanding user consent.

However, the GDPR goes on to be very specific about how to secure that data. With over 18 years safeguarding data for multiple heavily regulated industries (including PCI DSS, which echoes much of GDPR), StrongKey has the expertise and technology to help you transition towards meeting or exceeding GDPR requirements.

DEFINITIONS

The GDPR's founding principles (laid out in Article 1) state that "This Regulation lays down rules relating to the protection of natural persons with regard to the *processing* of personal data and rules relating to the free movement of personal data," and also that "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the *protection of personal data*."

As you think about your business, there are three important definitions to note before addressing the specific requirements of GDPR:

Personal Data – Any information relating to a person who can be identified by name, ID number, location data, online identifier, or other physical/socio economic identity factor.

Processing – Operation[s] performed on personal data automated or otherwise, including collection, recording, organization, structuring, or storage; adaptation or alteration; retrieval, consultation or use; disclosure by transmission or dissemination; and restriction, erasure, or destruction.

Pseudonymisation – Making personal data no longer attributed to a person without addition information, where additional information is kept separately to ensure the data is not identifiable without authorization.

SPECIFICATIONS

GDPR is wide-ranging, complex, and even up for interpretation in some areas. But these regulations have significant teeth in the form of financial penalties for non-compliance. StrongKey can help your organization avoid data breaches and their associated penalties, while also complying with some of the most difficult parts of GDPR. We outline them in more detail on the following pages.

Article	Concept	What it means	How we solve for it
4.11	Unambiguous consent	Users must give specific, informed, and—most importantly—**unambiguous** indication of their agreement to process of their data.	With many applications and websites reliant upon passwords, it is possible to steal a user's credentials, pretend to be them, and give false consent. StrongKey can deploy the strongest alternative to passwords – FIDO2 strong authentication – such that user consent is consistently unambiguous.
4.12	Protection against alteration of data	A personal data breach, according to GDPR, is accidental or unauthorized destruction, loss, disclosure, access, or **alteration.**	StrongKey protects against alteration of data through deploying digital signatures for data integrity.
25	Data protection by design and by default	This article expressly mandates that technical and organizational measures be taken to ensure that **data protection principles are designed into the system** and that only necessary data is processed for each purpose.	StrongKey's security architecture is designed to help organizations ensure that they identify necessary data for processing and that the purpose for processing is clear. The accompanying documentation with StrongKey's products helps organizations demonstrate compliance to their chosen approved certification method. StrongKey products allow organizations to deploy the strongest possible means of data protection that Article 25 mandates: 1. We encrypt and tokenize data within customer applications, the strongest possible place. 2. We provide hardware-backed key management, with exclusive control of keys belonging to our customers. 3. We protect access to data through FIDO-based strong authentication – the strongest means of authentication, and available in password-free convenience.
30	Records of processing activities	Organizations must keep all records regarding who has access, the purposes for processing, categories of data and recipients, transfers of data to outside organizations, when data will be deleted, and **the documentation of the security measures taken by the organization**.	StrongKey provides documentation and automated logging of tokenized data throughput to give organizations a leg up when it comes to keeping records of processing activities. StrongKey products and associated documentation assist with demonstrating the technical security measures your organization has taken.

Article	Concept	What it means	How we solve for it
32	Security of processing	This article mandates that: organizations use **pseudonymization** and **encryption** for personal data (*see definition on front*); processes for testing security measures are in place; and that appropriate levels of account security are applied to users; as well as that data confidentiality, integrity, availability, and resilience are ensured.	Our Tellaro security appliance makes encryption and tokenization (a form of pseudonymization) easy for our customers. Even better, we protect data in the strongest possible place—the application itself—ensuring that even in the event of a network breach, your data remains protected.

SUMMARY

While the GDPR has almost 100 articles governing business processes relating to data processing, the most difficult concepts to grasp are the ones involving securing data. That's where StrongKey can help. For almost two decades, StrongKey has led the way in tokenization and encryption key management for highly regulated industries like payment processing. With very similar requirements, GDPR is an ideal fit for StrongKey's solutions, allowing organizations to rest easy while the data they are responsible for is protected securely and achieving compliance is one step closer

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
Durham, NC & Cupertino, CA
Phone: +1 408-331-2000 | E-mail: getsecure@strongkey.com | Web: strongkey.com