KEEPER®

# GDPR

## What It Means for Your Business and How Keeper Enterprise Can Help Your Organization

# GDPR Overview

The General Data Protection Act (GDPR) is considered to be the most significant piece of data protection legislation to be introduced in the European Union (EU) since the 1995 Data Protection Directive, which the GDPR replaced. The GDPR enhances the individual data privacy rights of EU citizens and places significant obligations on organizations that handle consumers' personal data.

*"The fundamental concept behind the GDPR is that individuals, not organizations, own their personal data, and as such, individuals have rights regarding the collection and use of that data."*

Keeper Security is committed to making GDPR a success.

Although the GDPR is a European law, it applies to any organization that sells goods and services or tracks the online activities of individuals located in the EU, regardless of whether the organization has a physical presence in the EU. This means that nearly all businesses, must comply with the GDPR – even if they have only one customer located in the EU.

Under the GDPR, EU Data Protection authorities can fine organizations up to 4% of their global annual turnover or €20 million, whichever is higher, based on the seriousness of the breach and damages incurred. The GDPR also provides a central point of enforcement for organizations with operations in multiple EU member states by requiring companies to work with a lead supervisory authority for cross-border data protection issues.

# GDPR Data Subjects

The GDPR makes reference to "data subjects." This refers to individual people as opposed to legal entities like corporations. For most businesses, data subjects include not just customers but also employees, contractors, vendors and partners. This paper shall use "data subject" and "individual" interchangeably.

# GDPR Personal Data

The GDPR regulates the processing of personal data belonging to individuals in the European Union, including data collection, storage, transfer or use.

In an effort to future-proof the GDPR, authorities define "personal data" very broadly:

> ***"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"***

Here are some examples of what EU data authorities would consider "personal data" under the GDPR:

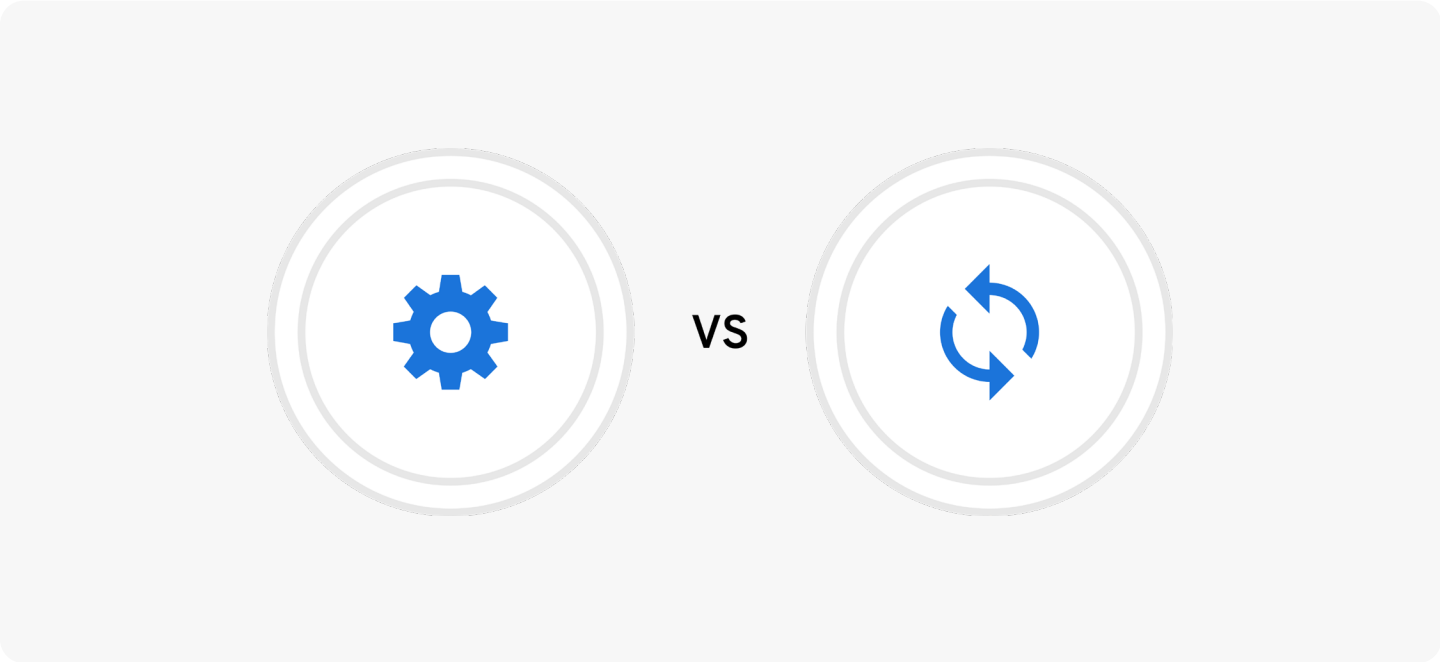
- An individual's name, address, personal email, business email, date of birth and phone number
- Online and device identifiers connected to an individual, such as IP address, cookies, MAC ID and RFID tags

Note that even if a single data point can't be used on its own to identify a specific individual, but it can be combined with other data to make the identification, then it is considered personal data.

# "Special Categories" of Personal Data

Article 9 of the GDPR places additional protections on "special categories" of personal data, including "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." Organizations are prohibited from processing this type of data except under specific circumstances as defined in Article 9.

Further, Article 9 allows EU Member States to "maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health."




# Data Controllers and Processors

Official authorities (i.e., governmental bodies like law enforcement) fall under another directive, but for all other organizations, GDPR identifies two entities that may process personal data:

1. A **data controller** decides what data to collect and what processing of personal data is done.

2. A **data processor** acts at the direction of the data controller to collect, store, retrieve and/or delete personal data.

Let's look at how this applies to Keeper Security specifically:

Keeper Security is a **data controller** when we sell our password manager directly to consumers. However, when we sell our password manager and other security software to organizations, we are a **data processor**, while the organization is the **data controller**.

# Lawful Purposes for Data Processing

As specified in Article 6 of the GDPR, data controllers must have a legal basis to process personal data. This includes:

- ✓ The individual data subject has given the organization consent to process the data
- ✓ Processing is necessary to fulfill a contractual obligation to the individual
- ✓ Processing is necessary for the data controller to fulfill a regulatory obligation
- ✓ Processing is necessary to protect the vital interest of the data subject or another natural person
- ✓ Processing is necessary to serve the public interest or "in the exercise of official authority vested in the controller"
- ✓ Processing is necessary to fulfill the legitimate interests of the data controller or a third party, except when "such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child"

It is essential that data controllers have clarity on and document the legal basis on which they are relying, as this legal basis directly impacts the data controller's responsibilities to the data subject.

For example, if the legal basis is consent, the individual may change their mind at any time and demand that their data be deleted, without having to provide any further justification. However, if the legal basis is to protect the vital interest of another natural person, an individual cannot have their data deleted simply by making a request. In such cases, the individual can challenge the legal basis. Only if the individual wins that argument may they then demand that their data be deleted.

"Legitimate interests" may seem like a tempting catch-all to avoid asking for consent. Rest assured that this is not the case. An entire analysis and justification must be done to demonstrate "legitimate interest." Such an analysis is performed in conjunction with legal counsel and is beyond the scope of this paper.

# Consent is Critical

**In most cases, organizations will use consent as their legal basis. Article 7 of the GDPR outlines four different conditions for consent:**

1. The data controller must be able to provide proof of the data subject's consent.

2. If the data subject's consent is given in writing as part of "a written declaration which also concerns other matters," the request for consent must stand out from the rest of the text and be written in "clear and plain language."

3. Data subjects can withdraw their consent at any time. Organizations must inform data subjects of their right to withdraw consent prior to the data subject giving it, and the organization must make it easy for them to do so.

4. Consent must be "freely given" by data subjects. Among other things, organizations cannot require that individuals consent to the processing of data that is not necessary to fulfill contractual obligations, including provisioning a service.

**Here's what these conditions look like in practice:**

- Individuals must freely opt in to having their data collected. This means no pre-checked boxes or any type of "assumed" consent.

    - A best practice is to provide individuals with multiple checkboxes: one to consent to data collection, a different box for every different purpose, a separate box to allow the data to leave the EU and a separate box to receive marketing communications.

- Organizations are prohibited from hiding opt-in information in walls of text, like terms and conditions, or writing it in confusing "legalese" instead of plain, layperson's terms.

- It must be as easy for individuals to opt out of data collection as it was for them to opt-in. For example, if the individual opted in on your website, you're not permitted to require them to send postal mail to opt out.

# Special Protections for Minors

Article 8 of the GDPR provides special protections for minor children, which the GDPR defines as anyone under the age of 16. However, EU Member States can lower this age to 13. Minor children cannot give consent on their own, consent must be given by a parent or other legal guardian, and it's the data controller's responsibility to ensure this happens.

# Data Subject Rights

The heart of the GDPR is to protect the rights of individuals in regards to their personal data.

### Right of Access

Article 15 discusses the right of an individual to have access to their personal data. This includes the data itself, purpose of the processing, category of personal data, where the data is located (third parties, moved to other countries), how long the data will be kept and/or the criteria to determine that timeframe.

Data controllers are additionally required to inform individuals of their rights to access their data, rectify errors, delete their data and restrict or object to the processing of their personal data.

### Right to Rectification

Article 16 grants individuals the right to fix errors in their data.

## Right to Erasure

Article 17 gives data subjects what's known as "the right to be forgotten." Individuals can request to have all copies of their personal data deleted. If the legal basis the data controller relied on was consent, the individual is not required to provide any reason or justification. If the data controller relied on another legal basis, the individual can still have their data deleted, but they must provide a reason, such as the original purpose for collecting the data is no longer valid, or the data was unlawfully processed.

## Right to Restriction of Processing

Article 18 allows individuals to restrict the processing of their data short of having their data deleted (in this case, storage is exempted from the definition of "processing"). There are several bases on which individuals can restrict processing, including:

- The individual's data contains errors, and processing should be suspended until the errors are corrected
- The processing is unlawful, but the individual wants their data preserved
- The controller no longer needs the data for processing, but the individual needs it preserved for legal reasons

## Controller Notification Obligation

Article 19 states that organizations notify data subjects of any changes to their personal data or how it's being processed.

## Right to Data Portability

Article 20 gives individuals the right to request that a copy of their personal data be provided to them or sent directly to another data controller in a structured, commonly used machine-readable format.

## Right to Object

Article 21 allows an individual to object to the legal basis for processing data that the controller asserted. It is then up to the controller to prove that they have the grounds to continue.

If the purpose of the data processing is for direct marketing, the data processing must stop.

## Right to Not Be Subject to Automated Decisions

Article 22 allows individuals to object to automated profiling or decision-making when the results of the profiling has legal or other significant effects on them. In some situations, the individual isn't able to stop the automated profiling. However, the individual still has the right to request human intervention and express their views on the profiling.

## Communication of a Personal Data Breach

Article 34 compels data controllers to notify individuals of breaches involving their personal data "without undue delay" in cases where the breach "is likely to result in a high risk to the rights and freedoms of natural persons."

This is not defined as a "right" but has the same effect.

# Responsibilities of Data Controllers and Processors

Successful compliance with the GDPR requires the participation of the entire company, including not just the legal and IT departments but also marketing, human resources, security and compliance and upper management.

## Personal Data Mapping

Though the GDPR doesn't explicitly require organizations to map their data, if organizations don't know what data they have, they will be unable to comply with data subjects' requests to provide copies of their data, correct errors, delete their data and so on.

## Metadata

Data controllers and processors must keep detailed and accurate records regarding the legal bases (Article 6) for collecting and processing personal data. If the legal basis is consent, organizations must be able to prove how and when the data subject provided consent (Article 7) and how the data was collected (directly or through a third party).

Article 30 requires data controllers to keep detailed, specific records of data processing activities, including the names and contact details for the controller, joint controller and processor; a list of categories of recipients to whom the personal data has been or will be disclosed, including recipients in other countries; the purposes of the processing; how long the data is to be held and criteria under which it will be deleted; and a "general description" of the security measures being taken to protect the data.

## Data Protection Officer / Point of Contact

Article 37 addresses circumstances under which organizations must designate a data protection officer (DPO); specifically, public authorities (other than courts) and private-sector organizations with "large scale" data operations. What constitutes "large scale" isn't defined. However, even the smallest organizations should, as a best practice, appoint a designated point of contact to handle GDPR requests from data subjects.

Articles 38 and 39 go into detail regarding the expected qualifications and job duties of a DPO. The data controller or processor must publish the DPO's contact details and provide them to data protection authorities.

## Fulfilling GDPR Requests

Because the GDPR empowers data subjects to request that their data be provided to them, edited or deleted, and enables them to withdraw consent to processing, data controllers must have people and processes in place to handle all types of requests from data subjects, ranging from a simple copy request to a full-on challenge of the legal basis for processing an individual's data.

For example, Article 12 requires data controllers to provide a copy of a data subject's personal data and metadata within one month of the request being made. The first copy must be provided free of charge, although the data controller may charge a fee for additional copies to help prevent abuse. Organizations must also keep accurate records regarding the legal basis for processing an individual's personal data and be able to produce those records on demand.

It is easy to see that an unprepared organization could be quickly overwhelmed by GDPR requests. It is also clear that GDPR compliance is not a one-and-done task, but an ongoing part of business operations.

## Transferring Data Outside the EU

Articles 44-50 of the GDPR specify rules regarding the transfer of data to non-EU countries or international organizations. Examples include sending email from the EU to the US, outsourcing to a non-EU data processor, saving data to a non-EU file service (Box, Dropbox, etc), or even using a web form from a third-party marketing company located outside the EU.

## Impact Assessments

Impact assessments (Article 35) must be done on all new personal data processes, especially if new technology is involved, to determine if the new processing operation itself presents a "high risk" to the rights and freedoms of individuals.

## Data Breach Notifications

The GDPR requires organizations to report data breaches to EU data protection authorities within 72 hours (Article 33) and notify impacted individuals "with undue delay" (Article 34).

However, Article 34 also specifies that individual notification is not required if the breached data has been rendered "unintelligible to any person who is not authorised to access it, such as [through] encryption." Therefore, it is in organizations' best interest to use data processing systems that encrypt data both in transit and at rest, and where encryption keys are stored separately from the encrypted data.

## Data Minimization & Encryption

Articles 25 and 32 of the GDPR make it clear that personal data should be protected in proportion to the risks to the individuals, technology and costs involved to implement technical and organizational controls. Two major concepts are specifically highlighted: data minimization and pseudonymization (encryption).

Data minimization is a simple concept, although it can be difficult to implement in real-world situations. It's the idea that organizations should collect only as much data required to perform the task at hand, and no more. For example, organizations should not collect phone numbers from customers unless they are needed to provide the product or service the customer is purchasing.

The GDPR views data pseudonymization (specifically, encryption), as a critical step in protecting data. As mentioned above, Article 34 states that individual data breach notifications are unnecessary in scenarios where the breached data was encrypted, as encrypted text (also known as ciphertext) is useless to the unauthorized party without the encryption keys to decrypt it. For this reason, it is crucial to store encryption keys separate from encrypted data. Storing both ciphertext and encryption keys in the same database is akin to writing down a safe combination and taping it to the outside of the safe!

# Demonstrating Compliance with the GDPR

## The GDPR and ISO 27001

Article 24 of the GDPR specifies that adherence to codes of conduct and approved certifications can be used to demonstrate compliance. One popular certification is ISO 27001, an international standard for information security management systems (ISMS). There are many ways in which ISO 27001 can help organizations comply with the GDPR. Here are just a few examples:

- ISO 27001 requires organizations to keep an asset inventory, and the standard treats personal data as an information security asset that is subject to rules regarding storage, length of storage, collection and access, all of which are GDPR requirements.

- Both the GDPR and ISO 27001 require organizations to perform a data protection risk assessment of privacy risks and vulnerabilities.

- Obtaining an ISO 27001 certification requires organizations to undergo a third-party audit wherein they prove they are complying with all of their legislative and contractual requirements – including the GDPR.

- ISO 27001 contains extensive guidelines on technical access controls, including procedures for user provisioning, granting user access and performing access reviews. Passwords and other IT secrets must be properly secured regardless of how strong they are. These controls help organizations prove that they are taking the necessary steps to secure their data from unauthorized access as prescribed by the GDPR.

Undergoing an ISO 27001 audit can help organizations identify areas where they need to shore up their GDPR compliance efforts, as well as their information security as a whole.

## Least-Privilege Access

While data minimization means that organizations shouldn't collect data they don't need, least-privilege access means they don't give users (employees, contractors, vendors, etc) access to data they don't need to do their work. Role-based access control (RBAC) is often used to implement least privilege by defining the access employees have to data based on their job descriptions. When people change roles, their access changes based on that role. When employees leave the company, their access is immediately turned off, and the former employee's credentials are transferred to a system admin or another employee to ensure business continuity.

Least-privilege access prevents unauthorized users from accessing personal data, a key tenet of GDPR compliance.

# Keeper Security and the GDPR

## Zero-Knowledge Architecture & Security

Keeper's password manager is built from the ground-up on a zero-knowledge architecture, ensuring that the individual user is the only person who can access their data.

Zero-knowledge means that:

- Customer data is encrypted and decrypted at the device level (not on the server)
- The application never stores plain text (human readable) data
- Keeper's servers never receive data in plain text
- The keys to decrypt and encrypt data are derived from the user's master password
- Multi-layer encryption provides access control at the user, group and admin level
- Sharing of data uses public key cryptography for secure key distribution
- Data is encrypted on the user's device before it is transmitted and stored in Keeper's digital vault. When data is synchronized to another device, the data remains encrypted until it is decrypted on the other device

No one but the customer/end user can view the plain-text data in their Keeper vault -- not even Keeper's own employees. This is in perfect alignment with Article 34 of the GDPR. Even if Keeper were to be breached, threat actors would obtain only useless ciphertext.

Data at rest is encrypted with 256-bit AES in GCM mode. Keeper implements a multi-layered encryption system based on client-side generated keys. Record-level keys and Folder-level keys are generated on the local device which encrypt each stored Vault record (e.g. Password). For example, if you have 10,000 records in your vault, you also have 10,000 AES Record Keys protecting the data. Keys are generated locally on the device to preserve Zero Knowledge and to support advanced features such as record and folder sharing. Record and Folder Keys are wrapped by other keys, such as the Data Key and Client Key.

Full encryption details can be viewed on our Security Disclosure page.

More details about our encryption model can be seen here.

## Regular Security Audits

Keeper is the most secure, certified, tested and audited password security platform in the world. Keeper holds the longest standing SOC 2 and ISO 27001 certification in the industry. Keeper is GDPR compliant, CCPA compliant, FedRAMP authorized (Moderate Impact), and is certified by TrustArc for online privacy. Keeper is PCI DSS certified. Tenable is deployed to perform daily vulnerability scanning of Keeper's system infrastructure.

The Keeper website and cloud storage runs on secure Amazon Web Services (AWS) cloud computing infrastructure. The AWS cloud infrastructure, which hosts Keeper's system architecture has been certified to meet the following third-party attestations, reports and certifications: SOC 1 / SSAE 16 / ISAE3402 (SAS70), SOC 2, SOC 3, PCI DSS Level 1, ISO 27001, FedRAMP, DIACAP, FISMA, ITAC, FIPS 140-2, CSA, MPAA.

Not only do we implement the most secure levels of encryption, we also adhere to very strict internal practices that are continually audited by third parties to help ensure that we continue to develop secure software and provide the world's most secure cybersecurity platform.

## Hosted on AWS

Keeper utilizes Amazon AWS' hardened cloud infrastructure in multiple geographic locations to host and operate the Keeper Vault. Data at rest and in transit is fully isolated in a customer's preferred global data center. In other words, EU data stays in the EU. This provides customers with the fastest and safest cloud storage.

## No Additional Processing

Keeper will never mine customer vault data for any purpose. First, it is a matter of policy at the highest levels of Keeper that we are committed to customer privacy. Second, because of our zero-knowledge architecture, it is technically impossible for us to do so. This follows GDPR principles of both organization and technical policies to protect personal data.

## Data Control

Customers may export their data (in csv format), modify or delete their vault records at any time, complying with GDPR requirements that personal data may be transferred or deleted as soon as the data is no longer needed, consent is withdrawn or the legitimate business purpose changes. Because data subjects are able to self-serve their Keeper vaults, the data controller is relieved of a significant burden in GDPR compliance. Our zero-knowledge architecture ensures that the data is encrypted such that only the data subject can access and decrypt it.

## Compatible with Active Directory, Azure AD, SCIM and SSO

Keeper is compatible with all Microsoft Azure AD environments for SAML 2.0 authentication and automated provisioning with SCIM. Keeper applications (including Web Vault, Browser Extension, Desktop App and iOS/Android apps) are 100% compatible with conditional access policies. Keeper supports both commercial (portal.azure.com) and Azure Government Cloud (portal.azure.us) environments.

Integration with Azure Active Directory is documented here.

Keeper integrates with any SAML 2.0 compatible identity provider such as Microsoft Azure, Okta, Google Workspace (formerly G Suite), Centrify, OneLogin, Ping Identity, JumpCloud and more. We offer two different SSO implementations: SSO Connect Cloud and SSO Connect On-Prem. Both implementations provide Zero Knowledge encryption with seamless authentication for end-users.

More information on SSO Connect Cloud can be found here.

Keeper also integrates with on-prem Active Directory environments. The Keeper Bridge allows businesses running Microsoft Active Directory to integrate with Keeper for the automatic provisioning and deprovisioning of Users, Roles and Teams to Keeper. The Keeper Bridge is designed to use the Lightweight Directory Access Protocol (LDAP and LDAPS) to communicate with LDAP based Directory Services for the purpose of onboarding and offboarding users to the Keeper platform. Additionally, Keeper's Commander toolkit provides AD password rotation plugins that can be configured or customized to the customer's business needs.

More information on the Keeper Bridge can be found here.

Keeper also supports the SCIM protocol to provision users through modern identity systems.
See: https://docs.keeper.io/enterprise-guide/user-and-team-provisioning

## Admin Insight & Auditing

Keeper Enterprise provides insight into employee password strength, use of multi-factor authentication and compliance with other security policies. Keeper provides audit logs complete with timestamps and filters to enable rapid searches for anomalies, forensics or compliance reporting.

## Data Processing Agreement (DPA)

Customers that are in the European Union may want to sign a Data Processing Agreement (DPA) with Keeper Security. For more information on Keeper's GDPR compliance, or to download GDPR download data processing agreements, please visit: https://www.keepersecurity.com/GDPR.html

*Disclaimer: Please note that the content of this whitepaper should not be construed as legal advice. It is being provided for informational purposes only.*