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 European data protection legislation to be introduced in the European Union (EU) in 20 years and will replace the 1995 Data Protection Directive. The GDPR enhances EU individual's privacy rights and places significantly enhanced obligations on organizations handling data.

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

At Keeper Security, we are committed to making GDPR a success.

The provisions of the GDPR apply globally to any organization that processes personal data of individuals in the European Union, including tracking their online activities, regardless of whether the organization has a physical presence in the EU.

When GDPR goes into effect May 25, 2018, it covers all data already collected as well as data collected going forward. This will be quite a challenge for many legacy systems.

Under the GDPR, authorities can fine organizations up to either €20 million or 4% of a company's annual global revenue (whichever is higher), based on the seriousness of the breach and damages incurred. Also, the GDPR 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.

Personal Data and Data Subjects

The GDPR regulates the processing of personal data about individuals in the European Union including its collection, storage, transfer or use. The concept of "personal data" is defined:

> **"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;"**

The definition was purposely broad to be all-encompassing and future-proof, rather than provide a static list. But certainly an individual's name, address, personal email, business email, date of birth and phone numbers are included. Furthermore, online and device identifiers connected to an individual count, and examples of this are IP address, cookies, MAC ID and RFID tags. Even if a single item can't be tracked to a specific individual, but it can be combined with other data to do identify an individual, then it is considered personal data.

Sensitive personal data is defined in Article 9 as information about racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, health, genetic, biometric and sexual orientation. Processing of this type of personal data has additional caveats.

Also, within that definition above of personal information, "data subject" is mentioned. It refers to actual people as opposed to legal entities like corporations. For most businesses, data subjects include employees (and extensions such as contractors, vendor and partner employees, etc) and customers. This paper shall use "data subject" and "individual" interchangeably.

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. A data controller decides which data to collect and what processing of personal data is done. A data processor acts at the direction of a data controller to collect, store, retrieve and/or delete personal data. Keeper Security is a data controller when we sell our password manager directly to consumers. We are a data processor when we sell to business, who in turn would be considered the data controllers.

Lawful Purposes for Data Processing

Data controllers have to have legal basis for the collection and processing of data as outlined in Article 6. These include a) individual consent, b) contractual obligation to the individual, c) a legal obligation of the controller, d) to protect the vital interest of the individual or another natural person, e) processing is in the public interest and f) legitimate interests of the controller or third party.

It is essential that the controller have clarity on and document which legal basis they rely. This is because there is a direct impact to the responsibilities the controller has in responding to individual rights. For example, if the legal basis is consent, the individual may change their mind at any time and demand the data be deleted without any further justification. However, if the legal basis is to protect the vital interest of another natural person, the individual cannot have their data deleted simply by request. They still have the right to challenge if the legal basis is true. Only if they win that argument may they then demand the data be deleted.

Also, note that "legitimate interests" is a tempting catch-all for avoiding consent. Rest assured that it is not the case. An entire analysis and justification beyond the scope of this paper must be done to enable this legal basis.

Consent is Critical

Most legal basis will be on consent and is defined as follows:

> **'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;**

Article 7 provides the conditions for consent. Individuals have to opt-in, meaning they have to give clear unambiguous consent for the data controllers to collect and use their data. No opt-in information should be hidden in other text (like terms and conditions) and definitely no pre-checked boxes. Multiple boxes may be needed: one to collect the data, a different box for every different purpose, a box to allow the data to leave the EU and another box to receive marketing communications. Finally, it has to be as easy to opt-out at any time as is was to opt-in.

Children under 16 must have consent authorized by the holder of parental responsibility. Member EU states have the authority to lower this age down to 13.

Data Subject Rights

The heart of 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 the individuals of their rights to access the data, to rectify errors, delete the data and restrict or object the processing of their personal data.

Right to Rectification

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

Right to Erasure

AKA the right to be forgotten, Article 17 allows individuals to have all copies of their personal data deleted. If the legal basis the data controller relied on was consent, then no reason is required from the individual. If the data controller relied on another legal basis, then the framework is provided for the individual to have the data deleted based on other means such as the original purpose is no longer valid or the data was unlawfully processed.

Right to Restriction of Processing

Article 18 allows the individual to restrict processing, but not have the data deleted (in this case, storage is exempted from the definition of processing). Several reasons are given, such as the data is incorrect and processing should be suspended until it is corrected, the processing is unlawful but the individual wants the data preserved, or the controller no longer needs the data for processing, but the individual needs it preserved for legal claims.

Controller Notification Obligation

Article 19 states that any changes to the personal data itself or in its processing be reported to the data subject.

Right to Data Portability

Article 20 holds that the individual may request personal data they provided be transferred to themselves or directly to another controller using 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 is for direct marketing, the controller is not able to object.

Right to Not Be Subject to Automated Decisions

Article 22 allows individuals to object to automated profiling when the results of the profiling create legal or significant effects on them. Some situations do not allow the individual to stop the profiling but even then, they have the ability to request human intervention and express their view on the profiling.

Communication of a Personal Data Breach

Article 34 compels data controllers to communicate data breaches, without delay, that is "high risk" to the individual. This is not defined as a "right" but has the same effect.

Responsibilities of the Data Controller and Processor

GDPR will require upper management support and several departments to implement. Though the IT department is key to success, they can't do it alone. Finance, legal, compliance, marketing, public relations and human resources will all be necessary to work for GDPR compliance.

Organizational controls include documenting data processes that contain personal data, risk assessments, the appointment of a GDPR point-of-contact (usually a data protection officer), the appointment of a team and GDPR training to relevant employees. Technical measures include the appropriate use of tools for classifying personal data, identifying and blocking data breaches and encrypting or pseudonymization of personal data.

Personal Data Mapping

Though GDPR is not explicit in that all personal data must be mapped out within data controller and processor systems, compliance would be impossible without doing so. To rapidly and accurately communicate and respond to data subjects, the ability to identify, retrieve, edit and delete all copies of the personal data and metadata is fundamental to GDPR compliance.

Metadata

In addition to the personal data itself, data controllers and processors must track the purpose of having the data, the legal basis (Article 6) for collecting and processing the data, if the legal basis is consent, then the details of how and when the data subject provided consent (Article 7) and how the data was collected (direct or third party). Article 30 is effectively telling the data controller to enforce Article 15. It and requires controller, joint controller and processor contact information, any other recipients of the personal data, how long the data is to be held (or the criteria for when it will be deleted), any data transfers to third countries or international organizations, and security safeguards to protect the personal data.

Data protection officer, point of contact

Designation of a data protection officer (DPO) is outlined in Article 37. The only guidance that a DPO is required is if the data operations are at "large scale" However, it is difficult to see how even the smallest organizations could respond to the rights of individual under GDPR without at least a designated point of contact to handle requests. A DPO is expected have a set of expected skills in data protection. Article 38 says that they be independent from the organization, and Article 39 enshrines DPO tasks in overseeing the GDPR processes.

Processes and automated systems

Because of the all the rights GDPR endows on individuals, data controllers must have people and processes in place to handle all the individual requests and challenges. Article 12 outlines that the data controller must provide to the individual, within one month of the request and free of charge, a copy of any personal data and metadata. The data controller may charge a fee for additional copies to help prevent abuse, but despite this, it is easy to see that an unprepared organization could be quickly overwhelmed. It is also clear that GDPR is not a one-off task, but an ongoing part of business operations.

Processes must be put into place to handle every request from a simple copy to a full-on challenge of the legal basis for all company data. This means that the team must have all the proper records for justification of their legal basis for all personal data. If consent is required, then all corresponding consent records must be available and defendable. The capabilities to make changes or delete personal data must be available once the decision is made that there was a proper request.

GDPR has several articles (44-50) on the transfer of data to third countries or international organizations. This must be watched very closely across the entire company as it is easy to see how data could be transferred in an instant without proper oversight. Examples would be an email sent from the EU to the US, outsourcing to a non-EU processor or saving data to a non-EU file service (Box, Dropbox, etc). Even an EU website containing a form from a 3rd party marketing company outside the EU could be a violation.

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 is "high risk" to the rights and freedoms of individuals.

Processes must be in place for outbound communications. This includes notification of individuals of their personal data rights and responses to requests. Applicable breach notifications to authorities must be made within 72 hours (Article 33) and individuals "with undue delay" (Article 34). While "undue delay" will surely be a topic of discussion, it is clear that careful consideration must be done before an incident in determining when a breach is declared, who will be informed and what the communications will be.

An important caveat to Article 34 in the notification of a data breach. If the data has been breached, but has been rendered unintelligible through encryption, then individual notification is not required. This is a great endorsement of any data processing system that encrypts data in transit and at rest. It also requires a system where encryption keys are kept separate from the encrypted data.

Data Security

Once a business determines that personal data is required in any capacity, then GDPR makes it clear that personal data should be protected in proportion to the risks to the individuals, state of the art technology and costs involved to implement technical and organizational controls. This is stated in Articles 25 and 32. Two major concepts are specifically highlighted: Data minimization, and pseudonymization (encryption).

Data minimization is a simple concept to understand, although its implementation is more difficult. SImply put, it is the idea that only the data required to do the task at hand shall be collected and nothing more. For instance, do not collect a phone number if it is not essential in providing the service intended. Given all the effort that goes into justifying, collecting and securing this information, looking critically at every piece for relevance will save headaches in the long run.

Taking steps for the pseudonymization (or specifically, the encryption of data), is seen by GDPR as a critical step in protecting data. As mentioned above, Article 34, where individuals must be alerted to data breaches, may be avoided if the breached data was encrypted (ciphertext) and therefore useless to whoever obtained it. This is also going to be dependent on keeping the encryption keys separate from the data. If a database has both the encrypted data and the encryption keys, then there is no point of encrypting in the first place.

Beyond those two concepts, steps must be taken to ensure confidentiality, integrity and availability of the personal data. While the methods are not prescribed, in the EU, ISO 27000 is a family of documents for industry standards in data security. ISO 27000 is recommended to protect personal data as defined by GDPR and all other data the business needs to keep confidential.

One of the tenets of ISO 27000 is that there must be an inventory of assets. Management must then classify the assets by how critical maintaining their security is. GDPR makes it clear that the personal data of employees and customers is of primary concern. Businesses need to consider how much protection is required for other data such as marketing research and plans, roadmaps, intellectual property and contracts.

Another tenet of ISO 27000 is that a team and plan be put in place to define how the assets in the inventory shall be protected. Assets must be assigned ownership and access controls - both physical and technical - be put in place that is commensurate to the value of the data. The security plan has to define who the owners are and what access controls are put into place. Part of the plan should also be how to identify breaches, fix them and report to stakeholders. GDPR makes clear that authorities and data subjects are critical stakeholders, but the business needs to consider executives, shareholders, legal and public relations communications are guided by the right people with the right message in the appropriate time frame.

ISO 27000 has considerable guidance on technical access controls. Procedures for user provisioning, granting access and access reviews are outlined in 9.1.1 and 9.1.2. Secrets such as passwords need to be protected, have guidelines for how strong they are and how often they are rotated in 9.3.1. Section 9.4.3 Requires the use of a Password Management System. Data and networks that are especially sensitive should require a second factor beyond the password such as cryptographic means, smart cards, tokens or biometrics (9.4.2).

Least privilege is a similar idea to data minimization. Data minimization means don't collect data you don't need and least privilege means don't give employees (or contractors, vendors, etc) access to data they don't need to do their jobs. 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, then all access shall be turned off. There needs to be a way for those credentials to be transferred to another trusted admin for business continuity. All user access rights need to be reviewed periodically to ensure

In all access controls, proper logging needs to be in place for auditing. This enables reviews for suspicious behavior, forensics investigations and evidence of compliance.

Demonstrating Compliance

When an incident happens, and it most certainly will, the risks of data loss to individuals and the number of individuals affected are key components of potential fines. Regulators have shown in existing cases already that fines will further be determined by how serious the business took safeguarding the personal data. This starts at the beginning with documentation of clear justification of the legal basis for the collection and processing of the data and, if based on consent, then clear indication that the individual was well-informed in giving consent. Businesses must prove that they practiced data minimization, had employee training on handling the data, that they meticulously tracked the data and related events and enforced data security concepts like least privilege and encryption. Regulators will consider all of these factors in levying fines.

GDPR provides for authorities to create GDPR compliance programs in the future which will surely help define expectations and set industry standards. Until then, organizations must have comprehensive plans for protecting personal data based on the risks of the specific data they are collecting and best security practices in handling that data.

Keeper Security and GDPR

We are taking steps to make changes to our business processes and products to ensure that we will be ready for GDPR by May 25, 2018. We are making changes to our analytics systems to ensure anonymity for our EU customers and making changes to allow you to control your consent about how any personal data that may be collected about you may be utilized or stored. Customers that are in the European Union may want to sign a Data Processing Agreement (DPA) with Keeper Security. Please contact your account representative or customer support for further information on how to request a DPA. For general inquiries about how Keeper Enterprise can help your business with the protection of your organization's passwords, private information and sensitive digital assets, please contact sales@keepersecurity.com.

How Keeper Security Helps With GDPR

Zero-knowledge Architecture and Security

Keeper's password manager is built from the ground-up on the idea that the individual user is the only person that can access their data. This is in perfect alignment with GDPR principles and data protection requirements. All encryption is done on the individual's device(s). The data is encrypted in transit with Transit Layer Security (TLS) and stored in AES-256 encrypted ciphertext. By separating the data and encryption keys, no Keeper employee is ever able to access customer vault data. As per Article 34, if Keeper vault data were ever breached, the ciphertext would worthless to the attackers and therefore no notification would be required.

In addition to regular security reviews and tests, Keeper is SOC 2 Type 2 audited and certified annually.

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. This enables the GDPR requirements that personal data may be transferred or deleted as soon as the intended use is completed, consent is withdrawn or the legitimate business purpose changes. Because the data subjects are able to self-serve their Keeper vaults, the data controller is relieved of a significant burden in GDPR compliance. The data is encrypted such that only the data subject can access it, so no employees can even see it, let alone have the need to access it.

Role-based Access Control

The security concept of least privilege means that employees should only have access to the minimum amount of data that they need to do their jobs. This is most often accomplished with role-based access control (RBAC).

Keeper integrates with Microsoft Active Directory (AD) to synchronize with nodes (organizational units), teams and users. Once connected, Keeper enables role-based access control at any node. Those controls can be cascaded to all lower nodes if desired. These controls on the Keeper vaults include master password strength, rotation time, 2FA requirements, IP whitelisting and more. Keeper locks accounts that are terminated in AD and those accounts may be transferred to trusted admins. This gives IT admins control over data accounts and assets throughout the organization.

Admin Insight and Auditing

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

Business Sales

Americas & APAC
+1 312 829 2680

EMEA
+353 21 229 6011

United Kingdom
+44 20 3405 8853

Germany & DACH
+49 89 143772993

Iberia & Italy
+34 919 01 65 13

Ireland
+353 21 229 6020

Sweden & Nordics
+46 8 403 049 28

Netherlands
+31 20 262 0932

Support

Americas & APAC (Consumer)
+1 312 971 5702

Americas & APAC (Business)
+1 312 226 4782

EMEA (Business)
+353 21 229 6019

https://keepersecurity.com

sales@keepersecurity.com