DataKeep™

SecurityFirst™ Protecting Critical Data

Compliance Bulletin

GDPR and the value of DataKeep

The European Union's General Data Protection Regulation (GDPR) went into effect on May 25, 2018 and holds organizations accountable for protecting customers private data at all phases of its use including collection, processing, retaining and ultimately deleting. While an EU regulation, it has global reach as it applies to all organizations controlling or processing the personal data of EU data subjects and holds them responsible for implementing data protection processes that ensure the privacy of such data.

GDPR improves upon the former Data Protection Directive 95/46/EC by introducing one set of new privacy rules that every member state must implement (a requirement, not a directive) or be subject to significant non-compliance fines of up to 20M Euros or 4% of annual turnover (total revenue).

There are 99 articles defining what must be done to protect the personal data of EU subjects. Many of them are outside the scope of what a data-centric solution like DataKeep can impact, so the focus herein is on the specific Articles related to data protection. An organization's answer to GDPR compliance will most likely be comprised of documented processes, multiple software products and services that may include considerable professional consulting engagements.

This overview presents areas where SecurityFirst DataKeep can help support certain requirements of the General Data Protection Regulation ("the GDPR").

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 ON THE PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, AND REPEALING DIRECTIVE 95/46/EC (GENERAL DATA PROTECTION REGULATION)

ENFORCEMENT DATE

Article 99 - Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. **It shall apply from 25 May 2018.**

Article 83 - General conditions for imposing administrative fines

Synopsis: Listing the fines related to the Articles described within this overview.

1. Infringements of the following provisions, depending upon the circumstances of each individual case, shall be subject to administrative fines up to:

Article	Fine
Article 5	€ 20,000,000 or up to 4% annual revenue
Article 17	€ 20,000,000 or up to 4% annual revenue
Article 19	€ 20,000,000 or up to 4% annual revenue
Article 25	€ 10,000,000 or up to 2% annual revenue
Article 32	€ 10,000,000 or up to 2% annual revenue
Article 33	€ 10,000,000 or up to 2% annual revenue
Article 34	€ 10,000,000 or up to 2% annual revenue

GENERAL DEFINITIONS (RELATED TO THE DATA ITSELF)

Article 4 - Definitions

For the purposes of this Regulation:

1. 'personal data' means 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;
2. 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
3. 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;
5. 'pseudonymization' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
7. 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
8. 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
9. 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.;
12. 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Article 5 - Principles relating to processing of personal data

Synopsis: This article states that a minimal amount of personal data can only be collected for a specific purpose, and not otherwise further processed. It also states that personal data should not be kept for any longer than is necessary to achieve the original intent of the processing. Personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

DataKeep for Article 5

DataKeep addresses the most stringent compliance requirements across all industries with built-in data protection, data access processes, cryptographic policy enforcement, auditing and reporting capabilities, and integrated key management. DataKeep data access policies only allow access to decrypted data when authorized users are processing the data, while protecting and tracking any unauthorized access, use or other malicious acts. Its monitoring capabilities can document when data was collected, who processed it, and when it was deleted for audit purposes.

Article 17 - Right to erasure ('right to be forgotten')

Synopsis: This article states that a data subject shall have the right to obtain from a controller the assurance that personal data concerning him or her has been erased without undue delay. It could be for several reasons, but most cases will likely involve a withdrawal of consent.

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
    - Personal data is no longer necessary in relation to the purposes for which it was collected
    - The data subject withdraws consent on which the processing
    - The data subject objects to the processing
    - The personal data have been unlawfully processed
    - The personal data has to be erased for compliance with a legal obligation
2. If the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers processing the personal data that the data subject has requested the erasure.
3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
    - For exercising the right of freedom of expression and information
    - For compliance with a legal obligation
    - For reasons of public interest in the area of public health
    - For archiving purposes in the public interest, scientific or historical research purposes

Article 19 - Notification obligation regarding erasure of personal data

The controller shall communicate any erasure of personal data to each recipient to whom the personal data has been disclosed, and to the data subject about those recipients if the data subject requests it

DataKeep for Article 17 and 19

DataKeep file level encryption offers a ready means of destroying any personal data. With its transparent, built-in key management capabilities, all phases of key lifecycle stay in your control. Automated key creation, rotation, and revocation/shred conform to industry compliance requirements. When data is no longer required, the customer can revoke the encryption key from the DataKeep system, leaving the data encrypted wherever it is stored, without a key ever being available again for decryption. In addition, DataKeep can log when a key was deleted for audit purposes. Note- further actions might be required for information shared with processor entities not bound to specific terms regarding its use.

Article 25 - Data protection by design and by default

Synopsis: This article basically says that any data processor should be implementing security measures before, during, and after the private data is collected and processed. The process should not expose data in clear text until the moment it's needed within an application.

1. The controller shall, both at the time of determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, and to integrate the necessary safeguards into the processing
2. The controller shall implement appropriate technical and organizational measures to ensure that, by default, only personal data which is necessary for the specific purpose of processing is processed.

DataKeep for Article 25

DataKeep will encrypt any data-at-rest and protect it from the moment of creation or collection through and while stored on a server asset. DataKeep easily fits into existing security infrastructures, whether as a separate single-pane-of glass, or integrated into automation via REST API. DataKeep provides the ability for customers to implement data access policies that protect encrypted data from unauthorized access, use or other malicious acts.

Article 32 - Security of processing

Synopsis: This article calls for the use of data protection technology to ensure an appropriate level of risk is maintained by the processor. It mentions the use of pseudonymization or encryption to protect the private data.

1. Taking into account the state of the art, costs of implementation and the nature, scope, context and purposes of processing as well as the risk and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:
   - The pseudonymization and encryption of personal data
   - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
   - The ability to restore access to personal data in a timely manner in the event of a physical or technical incident
   - A process for regularly testing, assessing and evaluating effectiveness of these measures to ensure the security of the processing.
2. In assessing the appropriate level of security, it should be taken into account the particular risks that are presented by processing, from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored or otherwise processed.

DataKeep for Article 32

DataKeep allows customers to deploy agents that encrypt data at the volume-level or for additional granularity, at file-level. It also allows customers to securely leverage on premises or cloud based object storage with client-side encryption key and access control. The object store agent leverages cryptographic splitting to send shares of encrypted data to multiple object store locations or multiple Cloud Service Providers for resiliency and recovery.

DataKeep assures confidentiality, data privacy and protection against brute force attacks. The SPxCore™ technology combines cryptographic splitting with AES-256 certified encryption and internal key management certified by the National Institute of Standards and Technology (NIST) to be FIPS 140-2 compliant. DataKeep also takes full advantage of the AES-NI hardware acceleration available in most current processors for optimal performance.

The file and volume agents include a native backup and restore capability that provides the ability to copy encrypted data, including in your backup storage environment. With either a full or differential backup - it allows you to restore access to personal data in a timely manner in the event of a physical or technical incident.

Article 33 - Notification of a personal data breach to the supervisory authority

Synopsis: This article states that any controller must report any personal data losses 72 hours after having become aware of it to the supervisory authority, unless “the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.”

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification shall at least:
   - Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
   - Communicate name and contact details of contact where more information can be obtained
   - Describe the likely consequences of the personal data breach
   - Describe the measures taken or proposed to be taken to address the personal data breach

DataKeep for Article 33

DataKeep is a Data-Centric solution that provides two key factors: 1) Data Security with Access Permissions that protect the data in the event of a breach, and 2) Access Logging with forwarding to a SIEM analytic engine for near real-time awareness of potential infiltration risk and alerts. As a result, information protected by DataKeep is unlikely to result in dire risks for an individual if breached and if so, provides the auditability of successful protection.

Article 34 - Communication of a personal data breach to the data subject

Synopsis: This article states that the controller, in the event of a data breach, shall communicate the personal data breach to all the effected data subjects without undue delay. It also states that no notification is necessary if the lost data was rendered unintelligible (encrypted) to any person who is not authorized to access it.

1. When a personal data breach is likely to result in high risk to the rights and freedoms of natural persons, the controller shall communicate the breach to the data subject without undue delay.
2. Communication to the data subject shall describe in clear and plain language the nature of the personal data breach
3. Communication to the data subject shall not be required if any of the following conditions are met:
    - The controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption
    - The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize;
    - If it would involve disproportionate effort, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

DataKeep for Article 34

DataKeep provides the ability for customers to implement data access policies that protect encrypted data from unauthorized access, use or other malicious acts. With DataKeep, organizations will be able to assess requirements on notifying EU citizens about data breaches based upon the clause, “appropriate technical and organizational protection measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption.” This ultimately helps preserve brand equity and reduce customer losses.

The GDPR is centered around the concept that privacy is considered a fundamental human right, and most of the core Articles in the regulation support the individual. At a high-level, organizations need to support and be in compliance with several fundamental Rights:

- To know what data is collected, used, and how long it is stored
- To see data in a readable format and have errors corrected
- To have access to data in a portable/useable format
- To be forgotten and have all identified data deleted
- To be notified of a data breach in a timely manner

DataKeep protects sensitive data to avoid costly fines and reporting requirements while supporting personal data rights. DataKeep encryption and access policies specifically support Articles 33 and 34, which state that no notification is necessary if the lost data was rendered unintelligible (encrypted) to any person who is not authorized to access it and is unlikely to result in a risk to the rights and freedoms of natural persons.

SecurityFirst™ delivers advanced security solutions that build a firewall around your data to protect against ever increasing threats and to aid in meeting regulatory requirements such as GDPR, HIPAA, NYCRR and many others.

DataKeep™, our flagship product, serves as your data firewall by using advanced encryption, scalable hierarchical key management, extensive policy enforcement and monitoring of unauthorized access to deliver the highest levels of availability, resiliency and time to value. Security requires a layered approach and protection of the data itself is your last line of defense.

SecurityFirst™
Protecting Critical Data

For a product demonstration or more information contact:
sales@securityfirstcorp.com
888-884-7152
securityfirstcorp.com