What is the General Data Protection Regulation (GDPR)?

According to the European Data Protection Supervisor "The EU's data protection laws have long been regarded as a gold standard all over the world. Over the last 25 years, technology has transformed our lives in ways nobody could have imagined so a review of the rules was needed.

In 2015, the EU adopted the General Data Protection Regulation (GDPR), one of its greatest achievements in recent years. It replaces the 1995 Data Protection Directive which was adopted at a time when the internet was in its infancy."

"The EU says GDPR was designed to "harmonize" data privacy laws across all its members' countries as well as providing greater protection and rights to individuals. GDPR was also created to alter how businesses and other organisations can handle the information of those that interact with them. There's the potential for large fines and reputational damage for those found in breach of the rules."

Who does GDPR apply to?

"Any company that stores or processes personal information about EU citizens within EU states must comply with the GDPR, even if they do not have a business presence within the EU. Specific criteria for companies required to comply with are:"

- A presence in an EU country.
- No presence in the EU, but it processes personal data of European residents.
- More than 250 employees.
- Fewer than 250 employees but its data-processing impacts the rights and freedoms of data subjects, is not occasional or includes certain types of sensitive personal data. This effectively means almost all companies.

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

What types of privacy data does the GDPR protect?

- Basic identity information such as name, address and ID numbers
- Web data such as location, IP address, cookie data and RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

What is Data Sanitization?

According to the Data Sanitization Consortium, "Data Sanitization is the process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable. A device that has been sanitized has no usable residual data, and even with the assistance of advanced forensic tools, the data will not ever be recovered. There are three methods to achieve data sanitization: physical destruction, cryptographic erase, and data erasure.

Although data destruction and data sanitization have similarities in their approach, they are not the same. Data destruction does not include verification or certification of successful destruction beyond forensic recovery. This means that the chosen data destruction method has not been proven to remove data in totality, whether that target data is a single file or an entire drive.

Visit www.clarabyte.com to read our eBook on Data Sanitization Best Practices

EU GENERAL DATA PROTECTION REGULATION (EU GDPR)

SPECIFICATION	DATA SANITIZATION SIMPLIFICATION
Article 1, Section 17: Right to erasure ('right to be forgotten') **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: **(a)**The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; **(b)** The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; **(c)** The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); **(d)** The personal data have been unlawfully processed; **(e)** The personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject **(f)** The personal data have been collected in relations to the offer of information society services referred to in Article 8(1)."	Create, maintain, and store audit logs of data erasure events that can be referenced by the Data Protection Supervisor. The logs need to be accessible and tied to the requests for erasure from the data subjects.

Article 13: Information to the Data Subject

1. "Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) The identity and the contact details of the controller and, where applicable, of the controller's representative;
(b) The contact details the data protection officer, where applicable:
(c) The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) Where the processing is based on point… the legitimate interests pursued by the controller or by a third party;
(e) The recipients or categories of recipients of the personal data, if any;
(f) Where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers… reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. The controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
(b) The existence of the right to request from the controller access to the rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
© Where the processing is based on point… the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were

Once the data has met the end of its retention period, make sure the data location is tracked and accessible for erasure. Tamper-proof records of erasure prove compliance.

collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information."	
39. "...Personal data should be processed only if the purpose of the processing could not be reasonably fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted."	Inaccurate data should be rectified, or securely erased and a tamper-proof (digitally signed certificate of erasure) record must be kept.
Chapter 3, Section 3, Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing "The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Articles 16, 17(1) and 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it."	Provide a certificate of data erasure to the data subject. The tamper-proof (digitally signed certificate of erasure) provides that assurance.
Chapter 1, Section 5, Article 25: Data protection by design and by default **1.** "the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. **2.** The controller shall implement appropriate technical and organi[z]ational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing,	By "design and default" implies that data protections are integrated or 'baked in' to an organizations processing activities or business practices, from the design stage right through the lifecycle. Data erasure procedures for end-of-life data are required.

the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."	
Article 30: Records of Processing Activities **1.** "Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: **(a)**The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; **(b)** The purposes of the processing; **(c)** A description of the categories of data subjects and of the categories of personal data; **(d)** The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations; **(e)** Where possible, the envisaged time limits for erasure of the different categories of data [...]"	The data controller's contact information must be on the certified erasure reports.

Protect Personal Information of EU citizens with Clarabyte's Data Sanitization Solutions

Clarabyte's intuitive and flexible data erasure software allows highly regulated organizations to easily automate their data sanitization processes to improve security, eliminate the risk of human error when processing devices, and guarantee compliance with the General Data Protection Regulation(GDPR). Clarabyte's proprietary algorithm offers data erasure for the entire spectrum of hard drives and solid-state drives, with verification of successful erasure, and tamper-proof reporting. This unmatched level of control over data removal provides assurance that no trace of target data remains on a device and compliance is guaranteed.

Click here to learn more about ClaraWipe Pro.

References:

https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552662547490&uri=CELEX%3A32016R0679

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

https://www.datasanitization.org/