EU GDPR and Email

The EU General Data Protection Regulation (GDPR) is the new legal framework governing the use of the personal data of European Union (EU) citizens across all EU markets. It replaces existing national data protection laws, and comes into force on 25 May 2018. The GDPR will affect all organizations in the EU and around the world that control or process personal data of EU residents. The new data protection law is not sector-specific, unlike privacy laws in other parts of the world. The same requirements apply to small businesses and large multinationals of all sectors, with very few exceptions. Consequently, organizations of all types are affected by the new EU data protection law.

The complete text of the EU GDPR can be found at http://eur-lex.europa.eu/eli/reg/2016/679/oj.

What is GDPR? A summary

- Regulates when and how personal data can be gathered by organizations.
- Regulates the use and processing of personal data.
- Sets up organizational end technical rules for secure processing of the personal data.
- Obligates organizations to immediately notify persons affected (data subjects) and official authorities in case of a data breach.
- Affects all organizations that ”control” or ”process” personal data.
- The consequences of breaching EU data protection law escalate drastically under the GDPR, which sets the maximum fine for a single personal data breach at €20 million, or four percent of annual worldwide turnover (whichever of the two is greater).
- The regulation will dramatically change the data protection needs for and consequences of non-compliance in Finland.

IPRA Technologies Ltd., Valtakatu 51, Vapaudenaukio Technopolis 2, 53100 Lappeenranta, Finland.
© IPRA Technologies Oy Ltd. Lappeenranta, Finland 2017. All rights reserved. EEZY KEYZ® is a registered trademark of IPRA Technologies Oy Ltd in the European Union.

Defining *personal data*

According to EU GDPR **Article 4**(1), personal data is "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."

This broad definition covers all data from which a person can be identified, such as records that relate directly or indirectly to employees, clients, customers, students, etc.

Defining *controller*

According to EU GDPR **Article 4**(7), a controller is "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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." This can mean any organization that collects and processes data either by itself or through an outsourced service.

Defining *processing*

According to EU GDPR **Article 4**(8), a processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." Any organization dealing with personal data is considered a processor.

EU GDPR **Article 4**(2) defines processing as "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."

In short, anything that is done to, or with, personal data (including simply collection, storage and transmitting) is considered processing.

IPRA Technologies Ltd., Valtakatu 51, Vapaudenaukio Technopolis 2, 53100 Lappeenranta, Finland.
© IPRA Technologies Oy Ltd. Lappeenranta, Finland 2017. All rights reserved. EEZY KEYZ® is a registered trademark of IPRA Technologies Oy Ltd in the European Union.

Defining a *personal data breach*

According to EU GDPR **Article 4**(12), a personal data breach is "any 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.

Security of processing

Article 32 (1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the **controller** and the **processor** must implement **appropriate technical and organizational measures to ensure a level of security** appropriate to the risk, including, but not limited to, the following:

1. the pseudonymisation and **encryption** of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

(2): In assessing the appropriate level of security account must be taken in particular of the **risks** presented by processing, in particular **from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed**.

(3): Adherence to an approved code of conduct as referred to in Article 40, or an approved certification mechanism as referred to in Article 42, may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

(4): The controller and processor must take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

IPRA Technologies Ltd., Valtakatu 51, Vapaudenaukio Technopolis 2, 53100 Lappeenranta, Finland.
© IPRA Technologies Oy Ltd. Lappeenranta, Finland 2017. All rights reserved. EEZY KEYZ® is a registered trademark of IPRA Technologies Oy Ltd in the European Union.

Recital 83: In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such **as encryption**. Those measures must ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration must be given to the risks presented by personal data processing, such as **accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed** which may in particular lead to physical, material or non-material damage.

From **Recital 78**: The **protection of the rights and freedoms** of natural persons with regard to the processing of personal data **require** that **appropriate technical** and **organizational measures** be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller **must adopt internal policies and implement measures** that meet in particular the principles of **data protection by design and data protection by default**.

Remarks on the GDPR

With the GDPR, encryption becomes mandatory. Data must be encrypted at every opportunity, including **at-rest and in-flight**. This applies equally to public cloud storage, preferably using user-managed keys, not just those provided by the cloud provider.[1]

If personal data is encrypted throughout its lifecycle using strong and approved algorithms it can be taken out of scope of the GDPR. Article 32(1) sanctions encryption as an appropriate security technique. However, all end-points must be taken into account. **Personal data is personal data, no matter where it is held.** For example, if a mobile device that contains personal data is breached while travelling, this is considered as much a data breach under the GDPR as one affecting a database.

Does the GDPR affect your organization's email?

Does your organization use email to send messages or files containing personal data of your EU customers, employees, prospects or leads? The personal data could be as simple as names, addresses, email addresses, phone numbers, gender, nationality, social security numbers, credit card numbers, online identifiers (such as IP addresses), or factors specific to the physical, physiological, genetic, mental, economic or social identity of EU persons. In short, any data from which a person can be identified is

IPRA Technologies Ltd., Valtakatu 51, Vapaudenaukio Technopolis 2, 53100 Lappeenranta, Finland.
© IPRA Technologies Oy Ltd. Lappeenranta, Finland 2017. All rights reserved. EEZY KEYZ® is a registered trademark of IPRA Technologies Oy Ltd in the European Union.

considered personal data. If your emails or attachments contain this information, the GDPR affects you. Transmitting and storing personal data is considered processing.

EEZY KEYZ® and GDPR

To prevent infringement of the GDPR, organizations controlling or processing personal data **should implement** measures such as **encryption** to mitigate risks presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data that is being transmitted, stored or otherwise processed.

EEZY KEYZ® encrypts email and attachments end-to-end on PC, Android and iOS. The encrypted email and attachments remain encrypted also on the devices and on the cloud (your email server). This prevents the unauthorized disclosure of email data and attachments containing personal information and unauthorized access to personal data that is being transmitted or stored.

The EU GDPR is a complex entity but with EEZY KEYZ® organizations can ensure that all their email is compliant. It has been developed by the principles of data protection by design and by default, which the GDPR also highlights. Once EEZY KEYZ® is adopted in the organization, all organizational email is end-to-end encrypted by default.

Our Cross-Platform solution for PC, Android and iOS enables safe and compliant way of accessing and transmitting email data containing personal data also on smartphones and tablets. EEZY KEYZ® is an easy and affordable solution to ensure your email is secure and GDPR compliant.

If you want to avoid sanctions and penalties by ensuring that your organization's email will not be breached, contact us for more information:

EEZY KEYZ®

https://eezykeyz.eu

sales@eezykeyz.eu

IPRA Technologies Ltd., Valtakatu 51, Vapaudenaukio Technopolis 2, 53100 Lappeenranta, Finland.
© IPRA Technologies Oy Ltd. Lappeenranta, Finland 2017. All rights reserved. EEZY KEYZ® is a registered trademark of IPRA Technologies Oy Ltd in the European Union.