GDPR

White paper on General Data Protection Regulation

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

LEGAL WHITEPAPER

What are the key obligations for controllers and processors of personal data with the coming GDPR regulation and how should an organization go about becoming compliant.

DEFINITIONS

Controller is a person or organization which determines the purposes and means of the processing of personal data

Processor is a person or organization which processes personal data on behalf of the controller

Data subject is a person whose personal data is processed

VERISEC

TABLE OF CONTENTS

ABSTRACT

This paper studies the new GDPR regulation issued on April 27 2016 and which will apply from 25 May 2018.

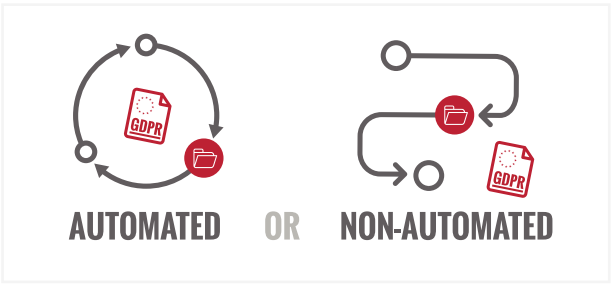
Any organization processing data relating to an identified or identifiable person, a so-called data subject, needs to comply with GDPR, and the consequences of not doing so can be substantial. Fines can reach 4% percent of the organization's global turnover, or up to 20 million Euros, whichever is higher.

There are a number of obligations imposed by GDPR on controllers and processors, and while the object of these rules is obvious, it can be hard to understand **how** to apply them directly to a specific organization or scenario. We will look at the key requirements, and offer some help in understanding the practical implementation of them. Included with this white paper is a practical GDPR checklist to help an organization get compliant.

> GDPR is a European wide regulation, and it is binding in its entirety and directly applicable in all Member States on May 25th 2018.

SCOPE OF GDPR

GDPR focuses on the processing of data by automated means but can also relate to data that forms part of a non-automated filing system.



Broadly speaking, anyone processing personal data about European citizens, whether or not the controller or the data processing is based in the EU or not, is subject to the GDPR rules.

BASIC PRINCIPLES

GDPR establishes some basic principles, which apply to personal data.

Firstly the data needs to be processed lawfully. In practical terms this means either that the data subject has **consented** to the processing of her personal data or that the processing is **necessary** for the performance of various legal obligations, whether the processor's or the data subject's. The definition of lawful consent is covered in a separate section below.

The data shall only be collected for specified, explicit and legitimate purposes. This is a principle called **purpose limitation.** Mapping data assets to a specific and legitimate purpose is therefore required.

Data minimization means that data processed needs to be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Beyond just linking assets to purpose, we therefore need to continuously establish whether the collected data passes the tests of adequacy, relevance and necessity and to cleanse the data if it does not.

Data needs to be accurate and where necessary, kept up to date and inaccurate data shall be erased or corrected. This is clearly a challenging task for any data controller, and one way of solving this would be to tag data assets or categories of as sets that are likely to change over time and establish a change process to refresh these data assets.

Data shall not be stored longer than necessary. This means that once necessity has expired as the basis of lawful processing, the data needs to be erased. If lawfulness is based on necessity, then it follows that the data assets should be tagged with the reason for that necessity, and a review process similar to the point on data accuracy above needs to regularly check that the lawfulness criterion is still fulfilled.

SOLUTION: Filter easily by tagging data

The controller needs to ensure the security of the personal data using both technical and organizational measures. **The regulation speaks of integrity and confidentiality of data, meaning that data has not been changed and that data is encrypted.** GDPR explicitly establishes that encryption be used to protect data assets, but just encryption is not enough. **Solid key management processes, policies and controls need to be in place to be able to demonstrate that data has not been lost, damaged or altered, destroyed or unlawfully processed.**

While encryption can only be achieved through technical means, key management could in theory be done with manual process, policy and controls. In reality however, with a complex mobile and cloud environment, an automated system that enforces key management policies, procedures and controls is essential.

CONSENT

Consent needs to be a clear affirmative act by the data subject. The regulation defines is as being a "freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her[1].

It can be a written or oral statement, it can even be ticking a box when visiting a website; **but silent consent, inactivity and pre-ticked boxes do not constitute consent.**

RIGHTS OF THE DATA SUBJECT

The data subject has a number of rights that are defined by GDPR. These rights pose some practical problems for the controller and processor in terms of quickly identifying and retrieving the relevant data assets in order to take a required action on them. Some of the key ones to bear in mind is mentioned below.

The right of access gives the data subject the right to find out whether personal data is being processed, the purpose of the processing, the category of the data, who the data will be disclosed to, the existence of any automated decision making based on the data and the period for which the data is expected to be stored. Controllers therefore need to add additional tags to the personal data in order to be able to quickly retrieve and present this additional information.

The data subject has the right to be forgotten, meaning the right to demand the erasure of data for which she no longer consents to data processing or which are no longer necessary to process. As mentioned earlier, this requires the controller to quickly retrieve an inventory of data assets and to establish which of these can be erased.

The right to data portability means that the data subject at any time should be allowed to receive, in machine-readable format, the personal data concerning herself. This right is also intended to make it possible for a data subject to move all personal data in a simple way to a new controller and data processor.

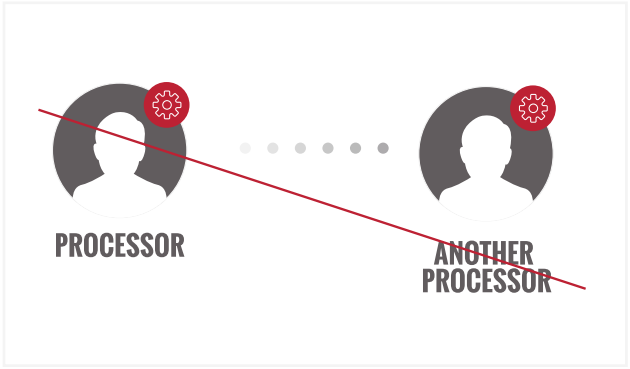
[1] (32) of the preamble to REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

RESPONSIBILITIES OF THE CONTROLLER AND PROCESSOR

GDPR details a number of responsibilities of the controller and processor. The key ones are mentioned below.

The processor shall not employ another processor without the controller's authorization. There are detailed requirements as to the contractual relationship between a controller and a data processor.

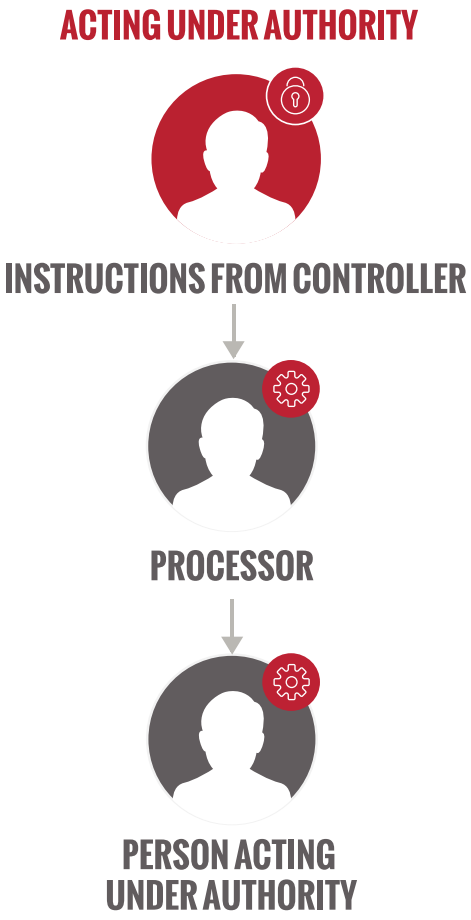
Controllers are required to keep records of their processing activities. Attached to this document is a template of the records required.



SECURITY

Controllers are required to ensure the security of processed data, explicitly through the use of encryption. The controller is required build its data processing by design and default on the basic principles, obligations and the rights of the data subjects as described in this white paper. This means for example that the system should be designed according to the principle of data minimization, in other words storing only data which is adequate, relevant and limited to what is necessary. Doing so will mitigate the liability in case of breach, and not doing so is in itself an infringement of the regulation and may lead to liability.

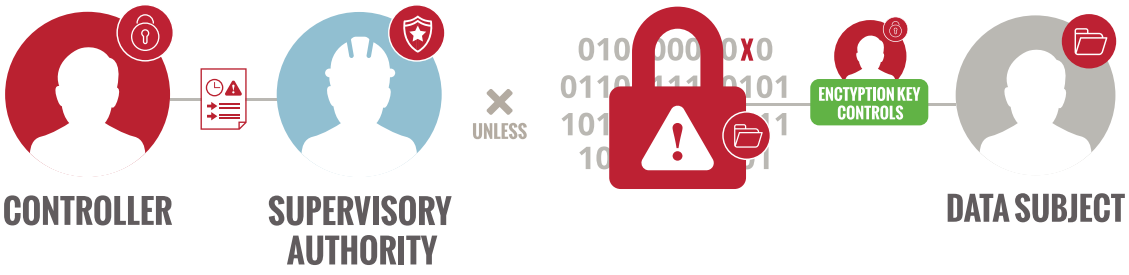
An important and explicit qualification is that the controller and processor shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller. This latter requirement can only reasonably be achieved through the adoption of solid key management practices and controls, either organizational or automated.



NOTIFICATIONS OF BREACH

In the case of a security breach the controller is obliged to report the 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. In practice this can be translated to mean that if the data is encrypted when the breach occurs, notification is not necessary[3].

The same principle as above applies to the obligation to notify the data subject as well. In both cases, the ability to determine that the breach is unlikely to result in a risk also depends on the encryption key controls that are available to the controller, since the value of an encryption system is no stronger than the encryption key management.

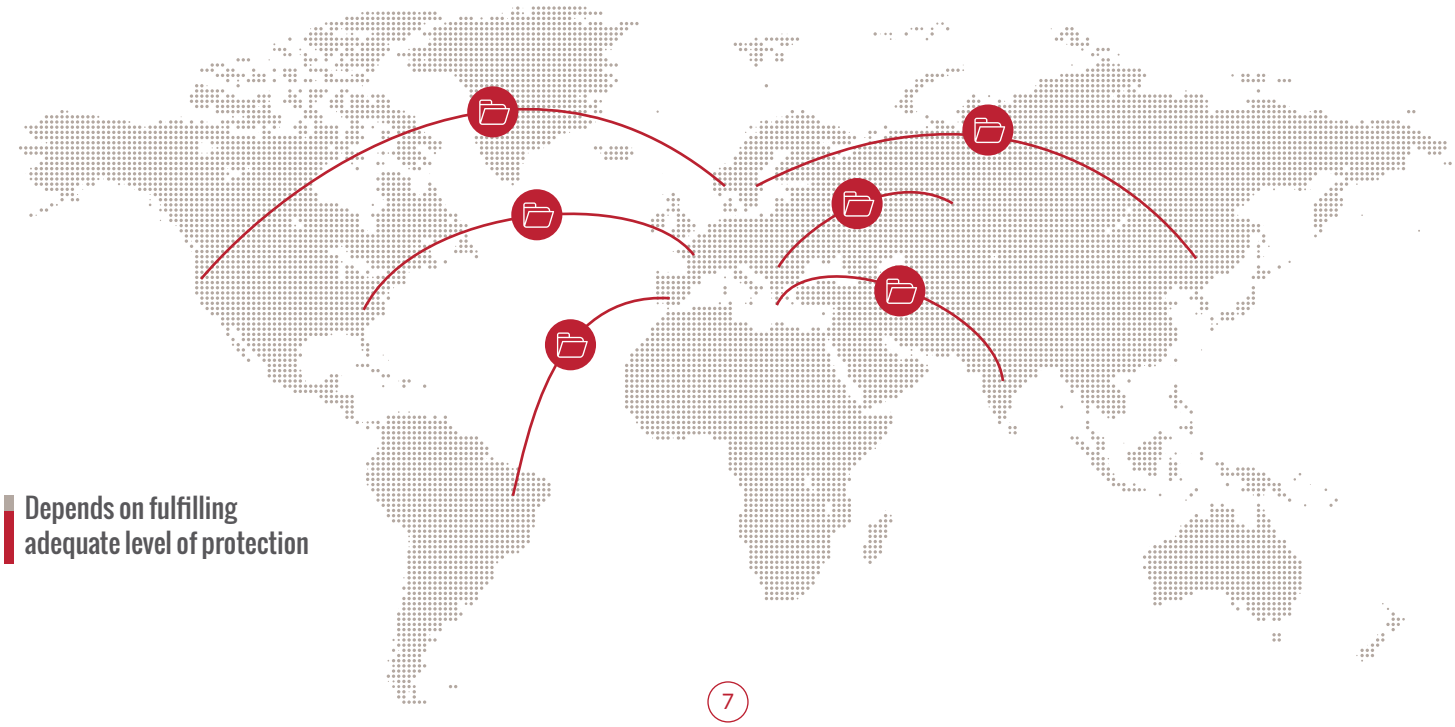


[3] While this exception is not stated explicitly, Verisec has sought an external legal opinion in this matter which confirms the claim that if the lost or stolen data is encrypted this excempts the controller from the obligation to notify.

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

The basic requirement for transfers to third countries is that the Commission has deemed that the country in question ensures an adequate level of protection. **The Commission shall publish in the Official Journal of the European Union and on its website a list of the relevant third countries.**

Any judgment of a court and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement between that country and the European Union.



Depends on fulfilling adequate level of protection

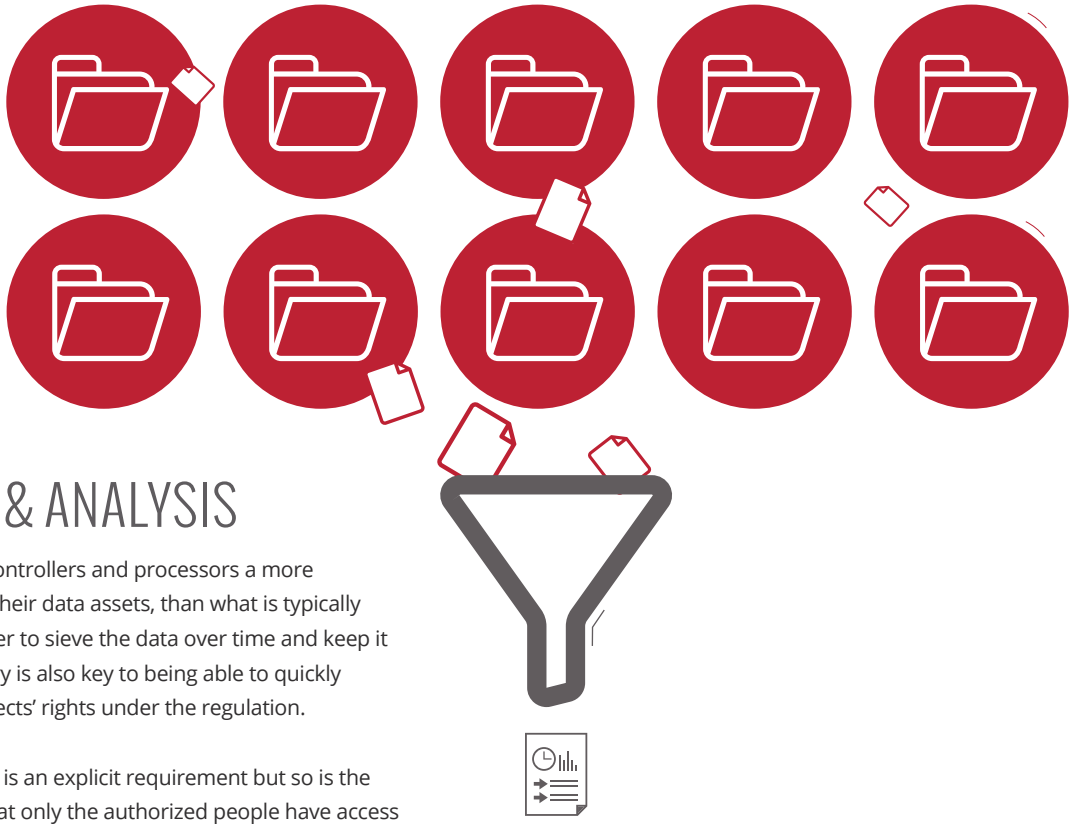
RIGHT TO COMPENSATION AND LIABILITY

Data subjects who have suffered damage from infringement of GDPR have the right to receive compensation for the damage suffered and any controller shall be liable for the damage caused by its processing.

The amount of liability will depend on the nature and gravity of the infringement and whether it was intentional or negligent as well as a number of other considerations. The key however to mitigating the risk of liability is the ability to demonstrate that action has been taken to comply with the basic principles and the general responsibilities of the controller.

The highest liability, the higher of 4% of global turnover or 20 000 000 EUR, is reserved for infringements of the basic principles, of the data subjects' rights and of the rules surrounding the transfer of personal data to third countries.

A lower liability, amounting to 2% of global turnover or 10 000 000 EUR, applies to lesser infringements including poor security design of the processing system.



SUMMARY & ANALYSIS

GDPR requires from controllers and processors a more granular inventory of their data assets, than what is typically available today, in order to sieve the data over time and keep it updated. This inventory is also key to being able to quickly comply with data subjects' rights under the regulation.

Encryption technology is an explicit requirement but so is the ability to determine that only the authorized people have access to the encrypted data. This is difficult and complex to achieve in through manual policy and procedure, automated systems that enforce policy digitally are therefore needed.

CONCLUSIONS

The key to compliance is to first make the effort to put in place a comprehensive inventory of data asset categories and a number of qualifier tags relating to time, lawfulness, purpose etc. that can be made easily searchable and made auditable. A template of the relevant data tags has been included below. **These tags need to be made easily searchable and auditable, and the underlying data needs to be erasable, changeable and moveable.**

Another key to GDPR is encryption and key management. An automated encryption and key management system that enforces key management controls, procedures and policies is likely the only way to comply with the regulation in an increasingly complex environment, with growing amounts of data and devices consuming and storing it.

VERISEC

Verisec is a technology provider in the areas of encryption and key management and of mobile Identity Management, ensuring that data is protected, and that only the right people have the keys to access their data assets.

About Verisec

Verisec is a company on the cutting edge of digital security, creating solutions that make systems secure and easily accessible.
The company provides a wide range of products and services within its two areas of business: Digital Identity and Information Security.
Verisec has global distribution and operations in Stockholm, London, Belgrade, Madrid, Frankfurt, Dubai and Mexico City.
Verisec is listed on Nasdaq First North in Stockholm since 2014.

www.verisec.com