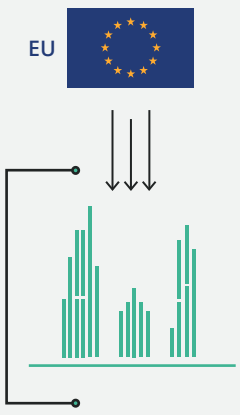
THE GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) is a regulation by which European authorities intend to strengthen and unify data protection for individuals within the EU. The GDPR also addresses export of personal data outside the EU, which means it targets companies that aren't based in the EU but process EU residents' data (UK included).

01 IF YOUR BUSINESS IS NOT IN THE EU, YOU WILL STILL HAVE TO COMPLY WITH THE REGULATION



Non-EU organizations that do business in the EU with EU residents' personal data should prepare to comply with the Regulation.

The **CONSEQUENCES** for failing to comply will be the same

02 THE DEFINITION OF PERSONAL DATA IS BROADER, BRINGING MORE DATA INTO THE REGULATED PERIMETER

Data privacy now encompasses more factors that can be used to identify an individual, such as their genetic, mental, economic, cultural or social identity etc.

Companies should take measures to reduce the amount of personally identifiable information they store, and erase it when no longer necessary.

03 CONSENT WILL BE NECESSARY TO PROCESS CHILDREN'S DATA

Parental consent will be required for the processing of personal data of children under age 16. EU Member States may lower the age requiring parental consent to 13.

04 CHANGES TO THE RULES FOR OBTAINING VALID CONSENT

The consent document should be laid out in simple terms. Also, silence or inactivity does not constitute consent.

Clear and affirmative consent to the processing of private data must be provided.

05 THE APPOINTMENT OF A DATA PROTECTION OFFICER (DPO) WILL BE MANDATORY FOR CERTAIN COMPANIES

ARTICLE 35 of the GDPR states that DPOs must be appointed for all public authorities.

In addition, a DPO will be required where the core activities of the controller or the processor involve regular and systematic monitoring of data subjects on a large scale or where the entity conducts large-scale processing of special categories of personal data.

06 THE INTRODUCTION OF MANDATORY PRIVACY RISK IMPACT ASSESSMENTS

A risk-based approach must be adopted before undertaking higher-risk data processing activities. In order to analyze and minimize the risks to their data subjects, data controllers will be required to conduct privacy impact assessments where privacy breach risks are high.

07 NEW DATA BREACH NOTIFICATION REQUIREMENTS

Data controllers will be required to report data breaches to their data protection authority unless it is unlikely to represent a risk to the rights and freedoms of the data subjects in question.

72 HOURS The notice must be made within 72 hours of data controllers becoming aware of it.

08 THE RIGHT TO ERASURE

"right to be forgotten"

DATA SUBJECTS NOW HAVE THE

A phrase made famous by the European Court of Justice ruling against Google Spain in 2014. The Regulation provides clear guidelines about the circumstances under which the right can be exercised.

09 THE INTERNATIONAL TRANSFER OF DATA

Since the Regulation is also applicable to processors, organizations should be aware of the risk of transferring data to countries that are not part of the EU.

Non-EU controllers may need to appoint representatives in the EU

10 DATA PROCESSOR RESPONSIBILITIES

Data processors will have direct legal obligations and responsibilities, which means they can be held liable for data breaches. Contractual arrangements will need to be updated, and stipulating responsibilities and liabilities between controllers and processors will be an imperative requirement in future agreements.

11 DATA PORTABILITY

Data portability will allow a user to request a copy of personal data in a format usable by them and electronically transmissible to another processing system. This aims to make users independent from any one company's services.

12 PRIVACY BY DESIGN

The GDPR requires systems and processes must comply with the principles of data protection by design and by default. Privacy in a service or product is to be taken into account not only at the point of delivery, but from the inception of the product concept.

13 ONE-STOP SHOP

A new one-stop shop for businesses means that firms will only have to deal with a single supervisory authority, not one for each of the EU's 28 member states.

PENALTIES

The GDPR mandates much tougher penalties than any previous national legislation. As a result, compliance with data protection legislation is now of utmost importance. Organizations can expect fines of up to 4% of annual global turnover or €20 million, whichever is greater. This makes the threat of insolvency or even bankruptcy very real.

LET iSERVER HELP

The GDPR will automatically enter into application on 25 May 2018. This leaves businesses little time to bring their operations to a state of compliance with the new law – especially larger ones. iServer comes with a preconfigured solution for companies that want to ensure they avoid risks. If you want to safeguard your company's interests, investing in a powerful solution such as iServer, take the first step towards achieving compliance. Our platform will empower your team by providing all the tools to design, build and manage a solid, comprehensive security architecture.