intetics
Where software concepts come alive

BECOMING GDPR COMPLIANT:

QUICKLY, EFFECTIVELY AND RISK-FREE

www.intetics.com

The abbreviation "GDPR" is becoming more and more often used in offices around the world. "GDPR" stands for General Data Protection Regulation, a new legislation approved by EU Parliament, which goes into effect in May 2018. As the date is approaching, discussions of how to achieve GDPR compliance is the hottest topic right now.

Generally speaking, the main goal of the new legislation is protection of freedoms and rights of all individuals that are located in the territory of European Union regardless of their citizenship. It builds up on previous pieces of data protection laws and presents a more thorough approach to the issue. GDPR takes into account accelerating world of international e-commerce and offers a more detailed and up-to-date set of norms for handling personal data of company's client base.

In many aspects, **General Data Protection Regulation** shifts the way we handle data and most importantly grants new powers to data subjects. It's necessary to emphasize that GDPR covers the protection of data of all individuals that are located in European Union. In practice, it means that every company, which collects data in European Union, must comply with the Regulation, even if company itself is not present in EU. Given the circumstances, it's safe to say that the GDPR makes a worldwide impact on how companies will handle data protection. It's also worth mentioning that expected penalties for those who won't comply with the GDPR are rather impressive – maximum penalty equals 20 million euro or 4% of annual worldwide turnover, whatever is bigger.

In such circumstances, every company should develop a cohesive risk management strategy and, most importantly, a compliance plan. Such compliance plan is an essential part of smooth transition that enables you to tackle all aspects of transformation in accordance with the requirements. It minimizes the risk of misconceptions and organizes the process in a comprehensive and achievable timeline.

Our company Intetics has already successfully adjusted to the new regulation and became fully compliant with GDPR. We would like to share some of the key points that would help your company to become compliant by May 2018 as well.

Learn Terminology

General Data Protection Regulation is a legal document, which means that it is written using specific terminology, the one we most likely don't use on a day to day basis. The body of the legislation consists of 11 chapters, 99 articles and nearly two hundred recitals. Needless to say that it is fairly lengthy and complicated, and requires certain preparation from the reader. To make the understanding easier, here are some main terms, used in the Regulation.

✓ **Term "personal data" refers to any information relating to an identified or identifiable person. An individual can be identified by name, an identification number, location data or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.**

✓ **Term "controller" describes any actor that determines the purposes and means of the processing of personal data.**

✓ **Term "processor" symbolizes a third party (vendor) that analyzes data in the ways, approved by the controller. It is controller's responsibility to ensure that vendors they cooperate with stick to the rules of the Regulation. In case vendors do not reflect the standards of GDPR, it is company's responsibility for cooperation with them.**

✓ **Term "data subject" refers to an individual whose personal information is being processed by controllers and processors. GDPR aims to protect rights of data subjects that are located in European Union.**

Ask For Consent

General Data Protection Regulation seriously considers how well-informed your customers (data subjects) are about what their information is ought to be used for. Companies are required to clearly state purposes of data collection, when and how it will be used and when destroyed. Company's desire to collect and process data should be explicitly stated, meaning that the will to collect data cannot be hidden along the lines of privacy policy or that data mustn't be recorded by default.

In order to ensure that the data processing is lawful, data subjects are asked to give consent to the usage of their personal information, unless the processing is necessary for compliance with a legal obligation, protection of interests of a data subject, performing a contract with the data subject or achieving the legitimate interests pursued by a controller or by a third party.

Know Their Rights

The new Regulation introduces some new and enforces already known rights of data subjects. From now on, individuals will have significantly more knowledge and power to control personal information, shared with the companies.

For instance, data subjects have the Right to Rectification or the Right to be Forgotten. Practically it means that at any point of time, an individual has the right to contact the company and ask to delete or change his or her information. According to the legislation, data must be modified or removed immediately, no longer than within a month upon the request of an individual. However, the Right to be Forgotten can be executed only if it does not contradict the legal system of data processing of a given country.

Individuals will have the power not only to withdraw consent to use their data, but to move it elsewhere. The Right to Data Portability enables customers to request a data transfer to a different controller. Basically, a customer can ask your company to transfer their data to a different (might be rival) company.

Some changes are introduced to the norms of notification. In case of a personal data breach - unauthorized disclosure of any data by a third party - an individual must be immediately notified. According to the GDPR, data subjects should be instantly notified about the loss or disclosure of any type of their personal information if it's expected to put under risk the rights and freedoms of a data subject.

Create a "Data Map"

In agreement with the Regulation, all controllers should comply with data minimization strategy, which dictates that companies are supposed to collect only necessary data to perform their services and reach an agreement with processor to destroy data as soon as the specific task was executed.

Companies have to demonstrate the conscious ways in which they handle data. Every question that customer survey contains should be justified and its purposes explained. Most importantly, a company should be able to present data protection methods that are used for ensuring data safety. Those include data encryption, usage of secure storage services and so on. Creation of a "data map" is an easy way to keep record of processing activities. The map could be created with the help of specific software or simple graphic editors.

Data maps are especially advised when it comes to working with personal data of your clients. It is important to include information about who in the company has access to specific data and at which stage of the processing. Mapping of data also helps to classify it as sensitive, confidential or public and track its flows. An important part of any map is monitoring cooperation with vendors as it is company's task to check that vendors also comply with GDPR and process data in accordance with your agreements. List of processors and details of agreements in order to easily review them should always be within your reach.

Do It Smart

It is always better to start the process of GDPR compliance with something simple. The best idea is to transform and improve your company's current data protection policies than invent new ones from scratch. Hence begin by auditing current process of data collection and review it according to the new Regulation. All units of the company should be involved in the transition and conducting educational and awareness trainings will teach employees to recognize data protection flaws and react to them.

As it was mentioned earlier, General Data Protection Regulation is a complicated legislation and it would be difficult to guarantee that all its criteria are met without proper legal advice. Thus, hiring an expert with knowledge of data protection in the field your company is working in, will be helpful in balancing the process. Intetics are happy to offer our services to your company and take a qualified initiative in making your company **GDPR compliant.**

After all, the more secure your company is, the more data your customers will be willing share, making your marketing campaigns precise and efficient.