NEW REGULATIONS ON PERSONAL DATA (GDPR)

– WHAT DOES IT MEAN FOR YOUR BUSINESS?

WEBCRM, SEPTEMBER 2017

Content

Overview 3

What is the GDPR? 4

Why is the GDPR so important for all companies? 7

How should my company approach GDPR? 8

CRM and the GDPR 10

FAQs 11

Overview

A new set of regulations regarding personal data is set to take effect on May 25th 2018. The law, which applies across the entire European Union, is officially known as the General Data Protection Regulation (GDPR).

The purpose of the new legislation is to give EU citizens better control over their personal data. This will be gained through a series of legal adjustments which lay down new and tighter requirements on how businesses handle and process personal data.

If you do not comply with the new GDPR legislation, your company may be fined up to 4% of its annual turnover.

As such, it is important for you to start looking at how you collect and use personal data for commercial purposes in your business.

As a CRM supplier, webCRM is, naturally, strongly focused on ensuring that our solution helps your company become GDPR compliant. Therefore, we are currently developing a process that aims to make this transition as simple and straight-forward as possible.

What is the GDPR?

On May 25th 2018, the new European Personal Data Regulation (GDPR) will enter into force across the EU.

The new legislation grants EU citizens greater control over their own personal data and requires that their information be handled securely all across Europe – regardless of whether the data processing takes place in the EU or outside the Union.

The GDPR is the EU's way of giving individuals, customers and suppliers more power over their own data. It also means fewer data processing options for the companies and organisations that collect and use data for commercial purposes.

When the GDPR enters into force on 25/05/2018, all individuals in the EU will have the following rights with regards to their personal data:

CLEAR CONSENT MUST ALWAYS BE GIVEN

Companies may not process an individual's personal data unless that person has voluntarily given specific, informed and unequivocal consent to this, either in a statement or by a clear affirmative action.

THE RIGHT OF ACCESS

This gives individuals the right to request access to their own personal data and to find out how their data is used by the company after it has been collected.

The company is obliged to provide a copy of all the personal data it holds on the person concerned, if that person requests it. The information must be provided free of charge and in electronic format.

THE RIGHT TO BE FORGOTTEN

If a person is no longer a customer of a company, or if they withdraw their consent for the company to use their personal data, they are entitled to have their data permanently deleted.

THE RIGHT TO HAVE DATA TRANSFERRED

Individuals are entitled to have their data transferred from one service provider to another. This must be done in a commonly used and machine-readable format.

THE RIGHT TO BE NOTIFIED

This right applies to any form of data collection carried out by a company. A person should always be notified before any data collection occurs. The person must give permission (opt-in) for their data to be collected. The consent must be voluntary and explicit – it must not be in the nature of implied consent.

THE RIGHT TO HAVE INFORMATION CORRECTED

This ensures that individuals can have their data updated if it is out of date or otherwise deficient.

THE RIGHT TO RESTRICT USE

Individuals may ask for their data not to be used in practice. Their data may be stored, but may not be used by the company.

THE RIGHT TO BE INFORMED

In the event of a breach of data security that could compromise an individual's personal data, the person has the right to be informed within 72 hours from the time when the breach is discovered by the company.

THE RIGHT TO OBJECT WITH IMMEDIATE EFFECT

There are no exceptions to this rule. All processing of data must stop as soon as a request is received. This includes the right to stop the processing of data for marketing purposes. This right must be clearly communicated to any individual whenever a dialogue is initiated.

Why is the GDPR so important for all companies?

The GDPR's fundamental aim is to create more trust and transparency between companies and EU citizens. Citizens should have confidence that the company that holds their data is using it in a way that they have agreed to.

As mentioned before, there are severe penalties awaiting any company or organisation that does not comply with the GDPR. They may be fined up to 4% of their annual global revenue or EUR 20 million, whichever is the greater amount.

In addition to protecting personal data, all companies and organisations that handle personal data are also required to appoint a data protection officer to ensure that the company complies with the GDPR.

How should my company approach the GDPR?

The GDPR is applicable whether your company's customers are consumers or other businesses. The legislation is based on the rights of the individual citizen – whatever the context in which that person's data has been recorded. Compliance with the GDPR is therefore equally important for all types of business.

As such, it is important for your company to establish clear guidelines, policies and processes for handling data. We advise your company to go through the following five exercises:

1. SAFETY FIRST

Be sure to develop and implement security measures throughout your infrastructure to guard against breaches of data security. It is crucial to establish a security system that can protect against data breaches and to act quickly and inform all relevant persons and authorities if there should be a breach of data security.

Be sure to also check your suppliers. Outsourcing services does not absolve you of responsibility. You must ensure that they also have the right security measures in place.

2. GET YOUR DATA DOCUMENTED

Get started as soon as possible with mapping all the personal data your company uses comes: Where does it come from? Examine where and how you store this information, and be sure to document how you use the data. You must identify exactly where all personal data is stored, who has access, and whether there is any risk of misuse or unauthorised access to the data.

3. PRIORITISE WHAT NEEDS TO BE STORED

Do not store more information than necessary, and delete data that is not used. If your business collects large amounts of data without any particular purpose or need, this cannot continue once the GDPR enters into force. The GDPR encourages more a disciplined treatment of personal data.

In the clean-up process, you should consider:

- Why are we storing this data?
- What do we aim to achieve by collecting these categories of personal information?

4. REVIEW YOUR DOCUMENTATION

When the GDPR enters into force, all individuals must actively consent to both the collection and processing of their data. You will therefore need to review all your data protection statements and adapt them where necessary.

5. BE SURE TO ESTABLISH PROCEDURES FOR HANDLING PERSONAL DATA

As discussed earlier, all individuals will have nine fundamental rights when the GDPR enters into force.

You should establish guidelines and procedures for how you intend to handle each of these situations:

- How can individuals give consent in a legal manner?
- What is the procedure if a person wants to have his/her data deleted?
- How will you ensure that this happens across all platforms and that the data is permanently deleted?
- How will you handle situations where a person wishes to transfer his/her data?
- How will you confirm that the person who asks to have their data transferred is who they purport to be?
- What is the communication plan in case of a data breach?

CRM and the GDPR

On 25/05/2018, all companies operating in the EU must have a plan in place for dealing with each of the nine data protection rights. Therefore, they need a system where they can store consents, partner agreements and customer data. Needless to say, webCRM allows you to handle this data in a GDPR-compatible CRM system.

We take the GDPR very seriously and are currently busy developing the necessary additions to webCRM, which will ensure that our customer have every opportunity to be fully GDPR-compatible on 25/05/2018.

Even now, our solution enables you to meet the vast majority of the GDPR requirements – assuming of course that your solution is configured properly. We will continuously update the solution so both you and we can comply with the GDPR before the new legislation enters into force. At the same time, we will do everything we can to make it as easy as possible for you to make the necessary changes. As such, we are working on integrating the GDPR directly into the user experience of our solution.

If you have any further questions about our work with the new Personal Data Regulation, please feel free to contact us. Alternatively, you can sign up for our monthly newsletter. Here we will provide regular updates on developments on the GDPR and guide you to how you may deal with these as a CRM user.

FAQs

When does the GDPR enter into force?
The GDPR was approved and signed by the European Parliament in April 2016. The Regulation will enter into force after a two-year transition period and, unlike a Directive, the GDPR does not require approval by the national legislatures. This ensures that the GDPR will enter into force in May 2018 across the EU.

Who will be affected by the GDPR?
The GDPR does not only apply to organisations operating within the EU. Organisations outside the EU are also required to comply with the GDPR if they offer goods or services to EU citizens. It applies to all companies that process and store personal data on citizens residing in the EU, regardless of the location of the company.

What are the penalties for non-compliance?
Companies can be fined up to 4% of their annual global turnover, or € 20 million, for breaches of the GDPR – whichever amount is the greater. This is the maximum fine that can be imposed for the most serious offences, such as where a company does not have sufficient customer consent to process data. There is a 'layered approach' to fines here: for example, a company may be fined 2% of its annual turnover for not having its records in order (Article 28), without informing the supervisory authority and the data subject of these omissions. It is important to note that these rules apply to both 'data controllers' and 'data processors'. This means that cloud companies are not exempt from GDPR enforcement.

What defines personal data?
Any information related to an individual or 'data subject' which can be used to directly or indirectly identify that person. This may be anything from a name, a photo, an email address or bank details to posts on social media, medical information or a computer's IP address.

What is the difference between a 'data processor' and a 'data controller'?
A controller is the agent who determines the purposes, conditions and means of processing personal data, while the processor is the agent who processes personal data on behalf of the controller.

Do data processors need 'explicit' or 'unambiguous' recorded consent?
The requirements for consent have been increased so companies will no longer be able to exploit long and 'unreadable' terms and conditions that are full of legal provisos. Going forward, the request for consent must be delivered in a comprehensible and easily accessible way. Consent must be clear and distinguishable from other matters, and should be provided in an understandable and easily accessible form, that uses clear and plain language. It must also be as easy to withdraw consent as it is to give it.

What is the difference between a Regulation and a Directive?
A Regulation is a binding legal act. A Regulation is applicable in its entirety throughout the EU, while a Directive is a legislative act that establishes a goal that all EU countries must achieve. However, it is up to the individual countries to decide how this shall be attained. It is important to note that the GDPR is a Regulation, unlike the previous law, which is a Directive.

Should my company appoint a Data Protection Officer (DPO)?
DPOs must be appointed for: 1) public authorities, 2) organisations engaging in systematic monitoring, and 3) organisations engaged in the processing of sensitive personal data on a large scale (Article 37). If your company does not fall into one of these categories, you do not need to appoint a DPO.