arriga crm
A MAREEBA GROUP COMPANY

General Data Protection Regulation - GDPR

A Practical Guide for SMEs

November 2017

GDPR

What is GDPR all about?

The General Data Protection Regulation (GDPR) is an evolution of the EU's 1995 Data Protection Directive. Consequently, in the UK, the Data Protection Act 1998 will be superseded by a new Act that incorporates the GDPR's requirements.

This guide to the General Data Protection Regulation (GDPR) is designed to help SMEs (Small and Medium Enterprises) take practical steps towards becoming compliant with the GDPR when it comes into force in May 2018. The guide is aimed firmly at SME organisations operating in the commercial and NfP (Not for Profit) sectors.

It applies to all organisations that deal with EU citizens regardless of where the organisation itself is located and will apply regardless of the outcome of the Brexit negotiations.

The GDPR has a special potential impact on SMEs for a multitude of reasons. Press headlines make much of the potential for very large fines to be imposed (€20m or 4% of global turnover) but there are other issues which might impact SMEs in particular.

If, as an SME, you deal with larger organisations, you need to ensure that the risk you hold in contracts does not equate to 4% of your large customer's revenues which may well be greater than €20m or 4% of your own turnover.

If you are an owner or operator of an SME, you will no doubt have an eye on the sales value of your business and this would undoubtedly be adversely impacted by falling foul of GDPR.

In addition, if you did fall foul of the GDPR, the time spent in dealing with the regulator both in terms of time and cost would be huge. Add to that the effort required to manage your reputation with customers and suppliers, and it is all too easy to imagine the scale of the commercial problem in addition to any penalty.

And finally, it would make the processes of raising capital even more difficult and expensive, given your new risk profile.

Major Penalties

The headline is that breaches of the GDPR will attract fines of up to €20m or 4% of global turnover and the stance of the regulator leads us to expect that actual fines imposed will be at the higher end of the range.

> ***'Breaches of the GDPR will attract fines of up to €20m or 4% of global turnover'***

If you are a smaller organisation contracting with a larger one, ensure that you are aware of any contractual risk that you might bear if you caused your customer to breach the GDPR. And don't neglect to consider the possibility of claims for damages from individuals in the event of a breach.

To put the severity of these penalties into context Talk Talk was recently fined £400K for a data breach but under GDPR this might well have been £73m. Similarly, Morrisons was fined £12K but their potential fine could have amounted to £640m.

arriga crm
A MAREEBA GROUP COMPANY

GDPR Overview

The GDPR replaces the Data Protection Act, comes into force on 25th May 2018 and affects all organisations that stores or processes data relating to EU citizens. This will include all categories of people that you deal with - customers, prospects, suppliers and employees. It extends rights to individuals and is founded on some key principles.

The Rights of Individuals

With GDPR, the rights of individuals are extended and can be summarised as the:

1. **Right to be informed** – when gathering data you must tell the individual what data you are collecting and the reasons why you are ` collecting it. This necessarily includes an element of how you will process it. The GDPR is very specific about the detail and timings of what you must do (see http://bit.ly/2viof3N).

2. **Right of access** – when an individual requests it, you must supply a copy of all the information you are holding about them within 1 month and without charge. Personal data includes any information that might identify an individual and includes cookie IDs and IP addresses.

3. **Right of rectification** – an individual has the right to have the information corrected.

4. **Right of erasure (Right to be Forgotten)** – an individual can request that information held about them is deleted if there is no compelling reason for the information to be held.

5. **Right to restrict processing** – if the individual objects or there is no need to hold data, then you may only hold sufficient data to identify the individual and ensure that processing is restricted.

6. **Right to data portability** – allows an individual to obtain their personal data, in an electronic (CSV) format, and reuse it for their own purposes across different services.

'GDPR comes into force on 25th May 2018'

7. You must inform individuals of their **right to object** to processing and direct marketing "at the point of first communication" and in your privacy notice.

8. Individuals have the right for a decision to be made by a human as opposed to a form of **automated processing** e.g. automated profiling.

GDPR Principles

The GDPR offers principles to guide us and which can be seen as placing obligations upon the processor. These "obligations" are:

- That processes are transparent. "It should be transparent [apparent to the individual] what data is collected and used, for what specific purposes, the existence and consequences of profiling, who is doing this processing, for what

time periods and who will receive the data…". This has potential important consequences for the way in which consent is gathered.

- Data can be collected for a specific legitimate purpose or with consent. If data is collected with consent, it should be understood that consent can be withdrawn. Therefore it is "better" for the organisation to establish a legitimate purpose for the processing of data. Of course, most organisations will have different sources of data e.g. customers, bought-in prospect lists etc. so it is important to segment the data to help with its management.

  Where the Processor relies on consent, it must be freely given, unambiguous, easy to withdraw and recorded.

- Data held is just sufficient for the purpose. Processors must be able to justify that they are holding no more data than is necessary for the stated purpose.

- Data is accurate and kept current.

- Data is not kept for longer than necessary for the purpose.

- The data is kept safe. This may be a small sentence but is potentially a massive issue. There are no prescribed standards but ISO 27001 is a good starting point.

- For those familiar with the Data Protection Act, these principles will be familiar. The most significant new principle is that of accountability. This requires that you be able to show how you comply with the principles – for example by documenting the decisions you take about a processing activity.

Overseas Data Transfers

If you transfer data overseas, compliance can be gained by introducing appropriate contractual clauses which may not be changed.

3 Questions you have to be able to answer

To start on the journey to compliance, you will need to be able to answer the following questions:

1. **What data do you have and how did you acquire it?**
   Does the information relate to customers, prospects that you were negotiating with, prospect lists, etc?

2. **Where is it?**
   You probably have a CRM system, indeed you may have several CRM systems or data repositories spread across the organisation. Where you have many customer databases, there is a risk that a person opting out in one system is still contacted because their details are held in another. Where do you store current and former employee information? Where do you store information about candidates who applied to your organisation?

3. **Is the data sent outside of the organisation?**
   If so, you will need to put in place specific contractual clauses that ensure compliance with GDPR.

ACTION REQUIRED

1. **Map your data processes**
   If you are to comply with the GDPR, you need to be in control of your data and be able to demonstrate that you are in control of it. If you cannot be certain how personal data enters your processes or what happens to it, you cannot comply with the GDPR and may be liable to a penalty.

   You also need to understand how data enters your organisation so that you segment data only once (see below). If you segment the information you hold but continue to let new potentially "non-compliant data" into your organisation, you will be analysing your data continuously.

2. **Segment your data**
   You will be able to process (use) certain information under the premise of legitimate interest. If you cannot use "legitimate interest", you will undoubtedly need to demonstrate that you have "consent". And you will certainly need to understand who has withdrawn their consent i.e. opted out.

   You can continue to contact and market to existing customers if you obtained their details during a sale (or process of negotiating a sale); are only marketing similar products or services and you have given and continue to provide an option to opt-out. This so-called soft opt-in does not apply to NfPs.

   For other sources of data, you will need to undertake a careful analysis of their sources and the permissions you gained when you acquired the data (also record when permission was given).

   The current Privacy and Electronics Communications Regulations (PECR) give clear direction on what to do if you have purchased a marketing list. You are required to know how and when consent was obtained, by whom and what the customer was told. Reputable sellers should be familiar with these questions and be able to respond properly. If they can't then you shouldn't use the data because you won't be able to demonstrate compliance.

You should maintain a 'suppression' list of people who have opted out. This should contain just enough information to identify individuals so they aren't sent marketing information in the future. By deleting data, you run the risk of adding them inadvertently to the database.

You must not use opt out or suppression lists to ask people if they still want to remain opted out. Such contact will likely breach the current DPA, certainly breach the GDPR and the PECR (if the contact was by phone, text or email).

3. Consent

The importance of consent has been made clear. Organisations should ensure that they keep clear records of exactly what someone has consented to. In particular, you should record the date of consent, the method of consent, who obtained consent and exactly what information was provided to the person consenting. There are a variety of ways in which this can be automated and it need not be onerous, but it must be done.

You should take action now to get the consents you need so that you can market to new people signing up today, after the GDPR comes into force.

4. Employment Processes

Many SMEs hold information about current and former employees and candidates spread across a number of systems including email. You need to centralise your data and ensure you have clear policies in place to control your information. This will require that you review all documentation including offer letters, handbooks, data management policies, privacy policies, monitoring of employees and appraisals and retention policies.

5. Implementation

To comply fully with the GDPR, you will need to introduce new processes across the organisation:

I. In the event of a security breach, you must notify the regulator within 72 hours. There are clear directions on what the notification must include, so don't wait for something to go wrong - build a template and a process for notification. Each breach must be documented with its effects and actions taken noted. If there is a high risk to individuals' rights and freedoms, then the individuals must be notified without delay.

> *'Record the date of consent, the method of consent, who obtained consent and exactly what information was provided'*

II. Privacy notices must be concise, transparent, intelligible and easily accessible; they must be written in clear and plain language. The ICO gives some examples of good and not-so-good notices (http://bit.ly/2iSx7Ft)

III. Contracts with Data Processors - there is a requirement for a written contract between a data controller and data processor, and existing contracts must be amended to incorporate

GDPR compliance. The controller must say how and why personal data is processed and the processor acts on the controller's behalf.

6. Data Protection Officer (DPO)

You must appoint a DPO if you are a public authority or carry out large scale processing. There are some special conditions that may require the appointment of a DPO who must be able to act independently.

The DPO has 3 functions:

- to inform and advise the organisation about complying with the GDPR
- to monitor compliance with the GDPR and other data protection laws
- to be the first point of contact for supervisory authorities and for individuals whose data is processed

It is recognised that small businesses with fewer than 250 employees won't have such detailed processes (there is a principle of proportionality) but exemptions are limited.

About Arriga CRM

Arriga was conceived by the team at Mareeba CRM Consulting who saw the need for a totally new sort of CRM implementation company.

Launched in 2016 to deliver the vision of a super-efficient CRM implementer, Arriga CRM delivers powerful, transformative results, quickly and cost-effectively. Staffed with some of the most experienced CRM people in the industry Arriga CRM operates as an independent company within the Mareeba group.

For more information about how Arriga CRM can help your company contact
Iain Kingsley on:
+44 (0)20 7692 7330 or email Iain at:
iain.kingsley@arrigacrm.co.uk