Serversys
Business Solution Experts

GDPR AND WHAT IT MEANS FOR CRM AND CUSTOMER ENGAGEMENT

A 7-step practical guide to achieving and maintaining GDPR compliance by **25 May 2018**

Contents

Introduction

Designed to empower all EU citizens to take greater control of their data, the General Data Protection Regulation (GDPR) will reshape the way organisations worldwide (who process data from the EU) approach data governance, data protection and privacy.

Despite the UK's decision to leave the EU, the government has confirmed that GDPR will form part of UK law and will come into force in 2018.

So, what does this mean for your organisation?

In a nutshell, any company that stores or processes personal information about EU citizens must comply with the GDPR.

The wide-ranging GDPR requirements that relate to how B2B and B2C companies process, store and protect customers' personal data include:

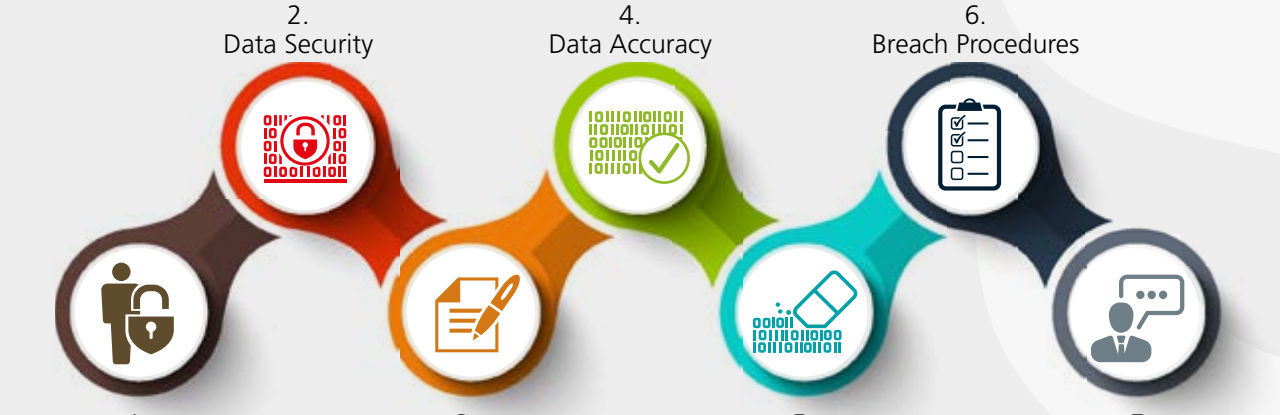
- *You can only store and process personal data after obtaining consent that is explicit – rather than implied*
- *All data must be freely given, rather than under the duress of not being able to access your services*
- *You have an obligation to allow individuals to see their own data, and to release a copy of any data you hold about them in a commonly readable format so that they can transfer data from one service provider to another*
- *An individual can demand all data be removed from your database – but you will have to retain their email address to ensure you do not re-import their information as a 'new' contact*
- *You must notify the relevant data protection authorities – in the UK this will be the Information Commissioner's Office - within 72 hours of a data breach, and any affected individuals if the breach affects their fundamental rights*

But that's not all. From the 25 May 2018 your organisation will not only have to comply with the GDPR – it will also have to be able to demonstrate compliance.

Failure to do so may expose your business to high fines – up to 4% of the annual turnover or 20 million Euros, whichever is higher – reputational damage, and/or loss of business opportunities.

This paper summarises a seven-step practical approach to achieving GDPR compliance with your CRM and marketing systems.

Our recommended seven cornerstones for GDPR compliance



1. Data Protection Officer

The GDPR will clearly create a significant data protection processing overhead on companies. The regulation also recommends that organisations establish a data protection function to manage this.

While not all organisations will need to employ a dedicated Data Protection Officer as initially feared, Article 37 of the GDPR states that organisations that need to employ a DPO are:

- *All public authorities*
- *Organisations where the core activities involve "regular and systematic monitoring of data subjects on a large scale"*
- *Organisations processing "special categories of personal data, such as personal, biometric or health data"*

For the business owner of customer data, this function should reside outside of the marketing division and IT as it's important that they take an independent view of data protection.

Even if your organisation isn't required to appoint a dedicated DPO, we'd recommend giving someone the role of "Data Protection Lead". As well as being responsible for ensuring privacy is at the heart of all that your company does, your Data Protection Lead will also report to the board.

While there is no qualifications requirement, we'd recommend the Data Protection Lead undertakes a 5-hour learning course as a GDPR Practitioner. Here's an example of an online provider we'd recommend for this type of training:
https://www.melearning.co.uk/

2. Data Security

Data security plays a prominent role in the new GDPR. For this reason, a good starting point for demonstrating compliance is to audit who has access to personal data and how data is used.

For example, do third parties have access? Do you have a separate e-marketing platform, or does data get passed through to third party systems?

If third parties are involved, you will need to ensure these are registered as Data Processors and are contracted to your GDPR policy. You will need to understand what the minimum requirements are for this contract, as outlined on page 16 of the ICO's publication Data controllers and data processors: what the difference is and what the governance implications are.

Other actions you will need to undertake include:

- *Review security and restrict access for those users who don't require data access. Limiting access to sensitive fields wherever possible demonstrates you have taken reasonable steps to secure your data.*
- *Limit the export capabilities of users in CRM if their role does not require such capability. You will need to document and regularly review who has this capability.*

2. Data Security contd

- *Audit emails so that if a data breach occurs, you can investigate effectively – for example, if a person leaving the organisation exports data from the system and sends it to an external address. If you don't have these audit capabilities, then consider moving to an email platform that does such as Office 365.*
- *Take steps to ensure third parties apply the same standards as you and restrict access to records that have positively consented to this third-party access. If you do share data with third parties, it's very important that when a contact opts in, you have a privacy notice that explains this and why. You will have to be crystal clear about who you are sharing the data with, and not just use generic words like Companies or Partners.*
- *You should ensure that you have a process for removing access quickly to employees if they leave your organisation or sooner, if you believe that they are at risk of misusing the data.*
- *Are the connections to your system secure? Ensure you regularly update your security measures like firewalls, two-factor authentication, anti-virus, and phishing protection. We recommend that you regularly train your employees on phishing techniques and consider stronger technologies to defend against these. An example of this is Microsoft Advanced Threat Protection.*
- *Are you able to remotely wipe devices and storage?*

Remember that you will need to demonstrate that you have taken all reasonable measures to secure data, so it's highly recommended to document all the steps that you have taken and ensure that you see this as an on-going process.

3. Consent

The GDPR considerably strengthens the conditions for consent and you will need to make sure that your organisation's email and marketing practices comply with the GDPR.

This means marketers need a clear affirmative consent action – you can no longer use a pre-ticked checkbox on a form, long rambling terms and conditions or soft opt-ins at in-store checkouts.

GDPR does not stop you from communicating with customers and clients where there are reasonable grounds to do so (legitimate interest). For example, sending commercial communications regarding the operation of the contract with them. However, GDPR does give people the absolute right not to receive marketing communications from you.

Your organisation will need to show 'provable consent' – a requirement that will call for more database fields to record proof of consent, the consent statement, the shelf life of the data, as well as when and where consent was obtained.

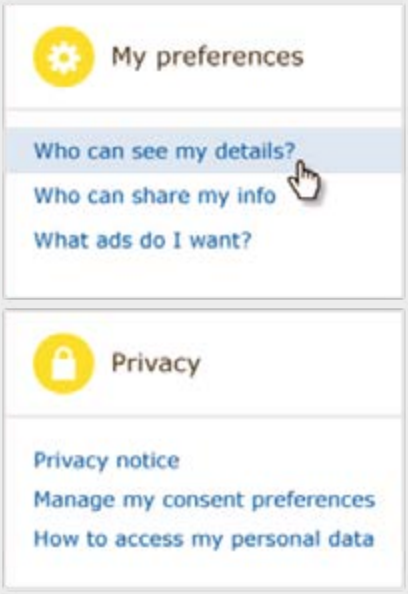
You should also note that:

- *Consent must always be freely given by the user and not bundled in with a contract.*
- *There must be clear opt-in capability to relevant information. You cannot have pre-ticked boxes and must be clear about what you are planning to do with the data (privacy notice).*

3.Consent contd

- *Users must have the capability to remove consent and you should make them aware of this prior to getting consent.*
- *You shouldn't assume consent is given forever. The ICO (Information Commissioner's Office) recommends that you ask for re-consent every two years.*

With this in mind, we recommend linking up e-marketing opt-in preferences with CRM, or even better using a preference centre web site that users can access to maintain their consent and see your privacy notice.



This consent should be audited, so you can demonstrate when and how someone's opted-in and what they were told you would do with their personal data.

Remember, you will need to ensure that consent is not be confused with terms and conditions.

B2B organisations should consider making sales and account managers review consent with clients, giving them the ability to manually send the consent email to encourage opt-in.

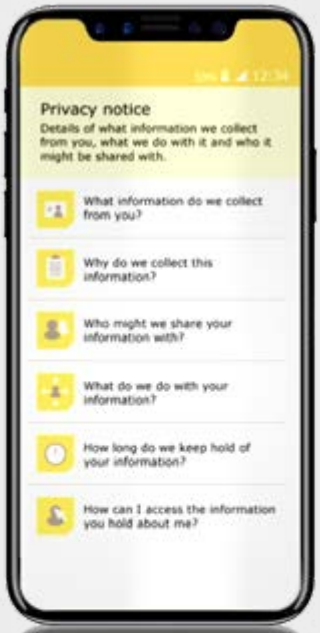
When marketing to individuals in businesses, ideally you should add consent fields to views and forms in your CRM, ensuring these are in prominent positions so that users can clearly see who has opted into what.

Consent can be given verbally, but this should be documented very carefully including the date time and specifically what a contact was told and consented to. This can be harder to record and as such we would recommend using an automated electronic approach as a failsafe.

Remember your obligation is to prove compliance and all the above steps will help you demonstrate this. Finally, you **cannot** rely on historic consent if this does not conform to the new GDPR requirements.

Some companies are concerned that not being able to blanket email prospects will have a detrimental impact on their marketing capabilities. But we'd suggest that this is a great opportunity to move your strategy to better digital platforms that may well generate greater success. Aim to start building an organisational culture that recommends people follow your digital channels, so that you expand your potential audience beyond data traditional methods.

You can download the ICO's consent checklist from here:
https://www.serversys.com/Consent_Checklist.pdf



Privacy Policy

Privacy by design or default is another key requirement of GDPR that will force a shift in how organisations think about personal data.

When collecting information on your website or any other means that contains personal information, such as an email address, you are required to share a very clear and concise privacy notice. This should cover at the minimum the following:

- *What information you collect*
- *Why you collect it*
- *Who you share it with*
- *What you do with it*
- *How long you keep it*
- *How individuals can access the information you hold on them*
- *Right to be Forgotten information*
- *How individuals can appeal to the ICO*

Your privacy policy should be in clearly understandable language, should identify by name any third parties you share date with and what these will do with it.

4. Data Accuracy

The GDPR accuracy principle requires companies ensure that personal data is accurate and, where necessary kept up to date. That means that every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.

Key actions to take to ensure your data is accurate include:

- *Removing any historic records from systems that are no longer required by your organisation.*
- *Implementing a process to ensure personal data is removed after a set period of time if there is no reason to keep it.*
- *Make sure that when you update a record, this change is also reflected on third party systems. For example, if you change someone's name you will need a process in place to update the accounts system, e-marketing tool and any other third-party systems of suppliers involved in working with you.*

Remember, data retention is a core consideration of GDPR compliance. Keeping stale records will increase your risk of non-compliance. Keep in mind that removing them will also limit your exposure if there is a data breach.

Using marketing lists

Does GDPR mean that you can't buy any marketing lists again?

No, it doesn't. But you will need to ensure that you have an adequate contract with the list provider and take all reasonable measures to ensure that the subjects have opted-in and are aware that you would be given their personal details in a way that is compliant with GDPR.

On the first communication to them or within a month, whichever is sooner of recording you should make subjects aware of the source of the information and give them the ability to amend their opt-in and see your privacy policy.

5. The Right to be Forgotten

GDPR introduces the right to be forgotten. That means that any individual has the right to request that their data is deleted from your records.

If you receive a request from a contact that they want their information deleted, you will need to have a process ready to handle this. This process should include reviewing if you have a contractual or legal reason to hold onto their data before you go ahead and implement the deletion request.

Anonymising records

If you anonymise a record, in other words, remove any reasonable ability to relate the data to a living person, then it is not subject to GDPR. You may wish to do this for reporting on things such as number of leads, where the actual data subject is not relevant. This anonymisation should be comprehensive, ensuring that no one can ever relate the record back to the person.

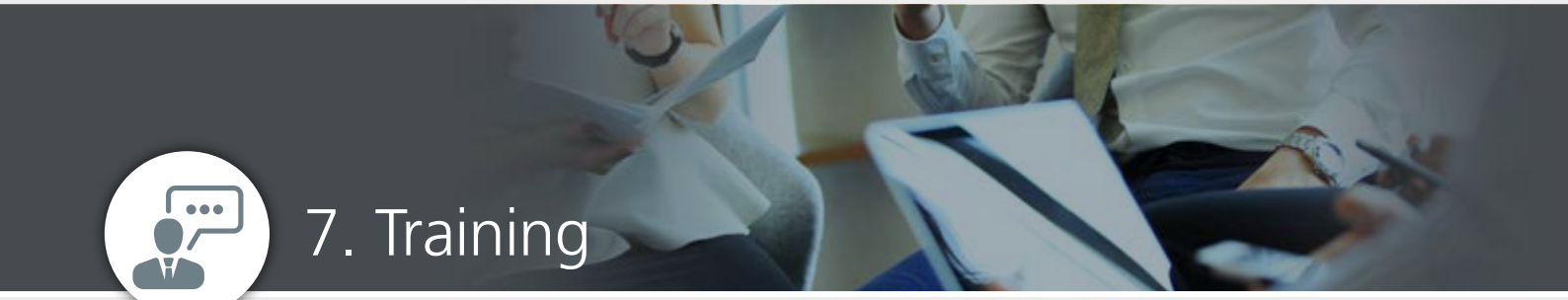
6. Breach Procedures

The GDPR introduces a much stricter regime for reporting data breaches. You are required to notify data subjects "without undue delay" and to inform the national data protection authority within 72 hours of a data breach being identified.

This means you will need to prepare a plan that kicks into action in the event of a breach, ensuring that marketing and communication teams are fully prepared for such an eventuality.

Your action plan should include:

- *Appointing someone who is responsible for the data breach investigation and reporting it to the supervisory authority.*
- *Reviewing the obligations of any third parties, such as an outsourced IT company, ensuring they are obliged to notify you in the event of a data breach taking place.*



7. Training

GDPR should be viewed as an opportunity to build good data governance and improve your marketing effectiveness.

Implementing the processes and procedures that relate to GDPR compliance will give you cleaner and more organised data, and ultimately better results.

For example, your e-mail campaigns will be more targeted to active marketing lists. Which will generate improved performance. You should also consider expanding your digital capabilities, making better use of platforms like LinkedIn and Twitter to compensate for any declining marketing capability that results from your GDPR compliance activities.

The final pillar of your GDPR efforts will be to ensure staff are fully trained on data policies and best practices for keeping customer personal data safe. You should also ensure they are trained to use techniques such as anonymisation.

Our recommendations include:

- *Use an online training platform for GDPR, where you can demonstrate that you have trained your employees on GDPR if you are audited. Online courses are available from online providers like www.melearning.co.uk/gdpr/courses.*
- *Build GDPR obligations into employment contracts, ensuring that staff understand why data protection is important, what personal data is, and the consequences of non-compliance.*
- *Build a company ethos of data protection, ensuring that everyone is aware of their individual responsibilities when handling personal data as part of their role.*

The Serversys Approach

We have appointed a Data Protection Lead with clear responsibilities who reports to the board.

Employees have GDPR responsibilities built into their contracts and GDPR training is mandatory. Consultants are required to pass a GDPR Practitioners course.

Our Data Quality and Consent Processes

All data that is stale has been removed from our CRM, Accounts and SharePoint systems where documents are stored.

We have emailed all our remaining contacts with a link requesting they opt-in to communications. These opt-ins clearly show what the purpose of the communications are, how their data will be used and where it is stored (Privacy Notice).

These links are unique for each individual contact, so when they land on our communication preference centre, the system knows who they are.

A contact can return to the preference centre, enter their email address and receive an email that has a link directly to amend their preferences (Consent).

All opt-ins are audited in our CRM system, so we know when a contact last consented or not.

Each new contact added to our system is automatically sent the opt-in email for consent.

Our account managers review any preferences that clients have not opted-in for and discuss the merits of opting-in with them directly. An account manager can send a link to the contact to amend their preferences.

After three months, any records where the client hasn't opt-in and where we do not have a commercial contract are considered for purging.

Based on when a contact last updated their opt-in preferences, every two years we will reset and resend a preference update request to contacts that have initially opted-in but have not transacted with us.

Our overall GDPR policy includes regular reviews of data security, breach and privacy plans.

We only use EU datacentres and monitor the security of these proactively.

Recommended Action Checklists

>> 25.05.18

Recommended Action Checklist ***Prior*** **to 25 May 2018**

> DATA AUDIT
- Is my data handled by Third Parties?

> PRIVACY NOTICE
- Do my data capture forms have a suitable privacy notice?

> REVIEW EXISTING CONSENT
- Does my current consent meet GDPR requirements? Review our helpful Consent Check List at https://www.serversys.com/Consent_Checklist.pdf.

> SECURITY
- Have you reviewed the security of your systems and removed unnecessary access and permissions?

> CONTRACTS
- Do your contracts with Third Parties cover the requirements for GDPR?

> PURGE
- Have you removed unnecessary data from your system?

> TRAINING
- Have you trained your staff and kept a training register?

> PROCESS
- Do you have appropriate processes in place should a data breach occur, or a contact wishes to exercise their right to be forgotten if required? If someone requests a copy of their records, can you do this efficiently in a timely way?

25.05.18 >>

Recommended Action Checklist ***Post*** **25 May 2018**

> TRAINING
- Do you have a process in place to train new and existing employees on GDPR?

> RE-CONSENT
- Put in place a process to manage re-consenting every two years.

> PRIVACY POLICY
- Review and keep reviewing.

> THIRD PARTIES
- Are they still honouring your GDPR policy?

> RISK
- Are your security measures up-to-date? Ensure you review access and permissions regularly.

> PRACTISE
- Playout a data breach, a right to be forgotten request and a request to see your records.

> DOCUMENT
- Keep all the measures documented so that if you are audited, you're ready and don't need to stress.

Other Resources

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

Need Help?

If you need help with GDPR or an advanced Preference Centre then why not get in contact and talk to one of our trained GDPR Practitioners.

Serversys
Business Solution Experts

www.serversys.com
+44 2038 843804
gdpr@serversys.com