Inter-com
Translations | Voice-overs | Interpreting

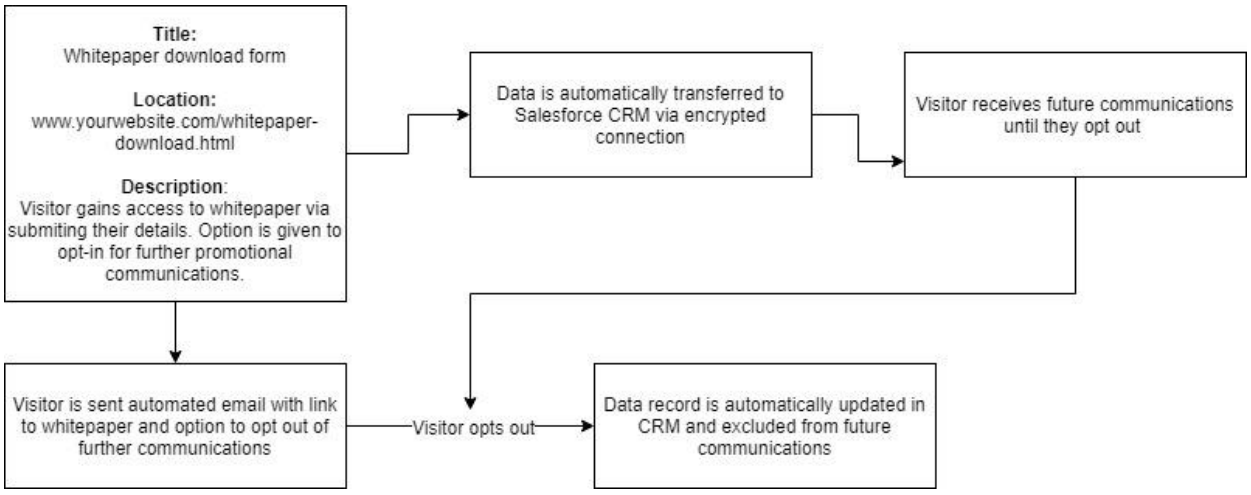
Your GDPR Compliance Checklist

On the 25th May 2018, the data landscape of the UK and Europe will change undeniably with the introduction of the General Data Protection Regulation, or GDPR. Many organisations, big and small, are trying to understand what this means for their business and how to best prepare.

The first thing to keep in mind is that like all legislation, there are areas in GDPR that are open for interpretation. Businesses are therefore left to assess their own vulnerabilities and hope to be able to implement suitable changes. With that in mind, we have rounded up the 'top level' GDPR requirements to help you become compliant. This is not meant to be replace a comprehensive GDPR audit but is meant to give you a good indication of the actions you will need to take.

1. Audit and document the flow of personal data coming into and out of your business

Do an audit and document where personal data is stored and what you typically do with it. This should be a fairly easy process for someone familiar with the company's processes but can be time-consuming if you have many different types of entry points for data coming into your possession. Below is a simple example of a data flow map:



You should also create guidance to ensure that staff are up-to-date on how to properly handle personal data and things they should avoid. A simple, hypothetical example of an item that could be included in this guidance: Before 'cold calling' a prospect in your database ensure that they have not opted out of future contact. Also ensure that they have specifically opted in to receive a sales call rather than a monthly newsletter. See next section for more on the topic of consent.

2. Review how you ask for individuals' consent

Consent is an important area of GDPR because if you are not compliant, it will be visible immediately. At all points where visitors are given the option to transfer their personal data to you (e.g. web enquiry forms, survey requests etc.) ensure that you include a mandatory request for consent to store and use the visitors' personal data in future. Below are some specific guidelines to keep in mind:

- **Make it visible –** consent requests should be clearly visible, transparent in their message and easy to understand.

- **Permission through action –** Individual should be required to give consent by taking an action rather than by being passive. For example by ticking a checkbox rather than leaving a checkbox unticked.

- **Give a reason** – Explain why you are asking for visitors' data and what you intend to do with it.

- **Be 'granular'** - If you have multiple ways of utilising a person's data, include an opt-in request for each. For example, include 3 separate checkboxes for giving consent to:
    - receive your company's monthly newsletter
    - receive your company's weekly sales promotion
    - share the individual's data with a 3rd party company

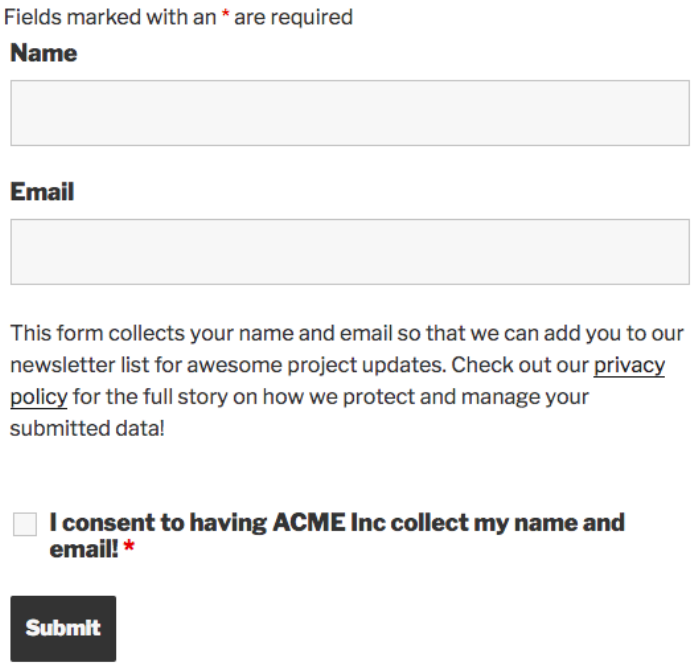
- **Be transparent about data-sharing** - If you have a commercial reason for sharing the personal data you control with a 3rd party, you need to state who this 3rd party is at the point of requesting consent. You also have to ensure that this partner is also GDPR compliant.

- **About withdrawing consent** – Let individuals know that they can withdraw their consent at any time and give brief guidance on how to do this. Ensure that individuals are not penalised in any way or receive a lower tier of service if they withdraw their consent.

- **Record and review -** Maintain a record that details how and when consent was given (keep in mind that in many cases this record is logged automatically). Periodically review that how you utilise personal data and whether it still matches the consent that users give.

- **Your pre-existing data –** if you are in possession of data that didn't meet GDPR's high requirements for consent, you need to seek consent again using the new standards or stop using the data.

Below is a typical example of a GDPR compliant web form:



3. **Check if your company needs to register with the Information Commissioner's Office (ICO)**

Take the ICO self-assessment to check whether you need to register with them to become GDPR compliant. This self-assessment is found here.

4. **Review your company's privacy policy**

- **Make sure you have one** – A privacy policy is a document that is freely available to the public and details how you store individuals' data, what you do with it and who you share it with. Although some of this information is included briefly when you ask for consent (see previous section), this is where you provide a more complete, detailed picture of how you manage personal data.

- **Make it readily available** – for example have a link to it on your website's footer where it's available from all your website pages

- **Make it easy to read** – use language that is age-appropriate and easily understandable by the layperson (i.e. the language should not be overly technical or legal in nature).

- **Review occasionally** – to ensure your privacy policy is up to date and always reflects your current practices.

5. **Giving individuals access to and the power to change their data**

- **The right to access** – If a person wants to know what data of theirs you are holding, you should have a process in place that gives him/her full visibility of this.

- **Include this process in your privacy policy**

- **Train your staff to deliver this process efficiently**

- **If you handle lots of data, automate** - If your organisation is large or handles a large volume of personal data, consider automating this access on a secure platform

- **The right of rectification, deletion and restriction** - have processes in place to give individuals the power to amend, delete or restrict the use of their data

- **Informing 3rd parties –** have a separate process in place to notify 3rd parties that have access to your data when there is a request made for the rectification, deletion or restriction of personal data

6. Automated data processing

Some business systems have the capability to process and act upon personal data though automated decision-making. An example of this is an automated follow up email being sent to a customer after they click on a certain link in a previous email.

Ensure that you have a process in place to change or stop this automated processes (via an actual team member if required) if and when this is requested by the data owner.

7. Your company's data protection policy

Write up a standalone statement that includes all your company's processes for ensuing the safeguarding of the personal data that you hold. A simple example of this is ensuring that staff know that they are only allowed to access their CRM from a device that is approved. Below are some points to guide you:

- **Document** - In your policy, include your company's approach to data protection and set out the staff's responsibility to ensure its safeguarding

- **Educate** – communicate the data policy to all your staff and make it part of on-boarding procedure for new staff

- **Review** - Periodically review this policy and ensure if reflects how the business operates in the present and is suitable for the systems it currently uses

8. Written contract with 3rd parties

Have a written agreement in place between you and any 3rd party that stores or processes data on your behalf that states that they do so in a GDPR compliant manner. You can use the Information Commissioner's Office (ICO) checklist, found here, as guidance when drafting new contracts for this purpose.

9. Data Security

When it comes to data breaches and network attacks, even major data controllers such as Equifax, Sony and Adobe (who presumably invest millions into their data security) have not been immune to being hacked and their data being stolen.

For this reason, GDPR compliance includes a requirement for companies to build good data security practices into their operation and to manage data risks responsibly. Below are some examples of strategies used to manage data risk properly:

Allocate the appropriate resources to data and network security – ensure there is someone proactively taking ownership of your network's security and mitigating its risks.

A typical example of this is a Network Manager performing a series of weekly actions such as: Patching the server operating system, checking the network firewall, performing vulnerability scans etc. Under GDPR, you would allocate periodic time and resources for training the Network Manager on the latest security practices.

Only store what you need and pseudonymise data where possible - minimise amount of personal data that you hold on any given individual. If possible, do not hold data that will help to identify a person by cross-checking with other publicly available data (for example their home address).

Data breach prevention – You should have processes and systems in place for preventing data breaches. Below are two simple examples of this:

- have an automated network policy that requires users to periodically change their CRM and PC logins
- Train staff on how to recognise and handle suspicious emails. Have this as part of onboarding process for new employees.

Data breach response – train staff on how to recognise, report and respond to data breaches

More information on network and data security can be found in the ICO's guidance index under the 'security' section.

10. The Data Protection Impact Assessment (DPIA)

Any project or activity that your company undertakes that involves personal data, should include a DPIA. This process should be assigned to someone who has influence or manages project processes (such as the Project Manager) and data protection actions should be included as part of the existing project plan with the appropriate resources and time allocated to them. For more information on the DPIA, click here.

11. Assigning a Data Protection Officer (DPO)

A DPO is a person in your organisation that is responsible for the correct management of the personal data that you store or process. His/her role is to assess and advise senior management and stakeholders on an ongoing basis and to ensure that the organisation is managing personal data responsibly, securely and in line with best practices.

Under the Information Comissioner's Office (ICO) you must appoint a Data Protection Officer if:

- *you are a public authority (except for courts acting in their judicial capacity);*
- *your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or*
- *your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.*