A fast and handy guide to GDPR

+44(0)141 273 7000 | innovationdigital.co.uk

With one month to go until the General Data Protection Regulations (GDPR) comes into force on 25th May 2018, we have summarised the most common questions our clients have about the new legislation.

What is GDPR?

The first GDPR text was published by the EU Commission in January 2012. The Commission wanted to update data protection law because there had been huge technological advances since the 1995 Data Protection Directive, particularly in the marketing sector. The law needed to consider new technological developments, the resulting proliferation of consumer data, and changing consumer attitudes and expectations.

Does the GDPR apply to my organisation?

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

If you collect and / or process any personal data, as defined above, relating to EU citizens (even if you are not based in the EU) then GDPR will apply to your organisation.

It's important to note that even B2B information that contains personally identifiable information (eg an organisational email address containing a person's name) is classed as 'personal data' and is covered by the GDPR.

What are the main changes as a result of GDPR?

This change in legislation puts much more focus and accountability in place for organisations to ensure they are handling personal data appropriately and in line with legislation.

The main themes of the changes are as follows:

Consent

Consent should be "freely given, specific, informed and unambiguous," with controllers using "clear and plain" legal language that is "clearly distinguishable from other matters".

Whenever a user is about to submit their personal information you have an obligation to make sure the person has given their consent. You will also be required to provide evidence that your processes are compliant and followed in each case. Previously, consent could be inferred from an action or inaction in circumstances where the action or inaction clearly signified consent. Thus, the Directive left open the possibility of "opt-out" mechanism. However that will change under the GDPR which requires the person to signal agreement by "a statement or a clear affirmative action."

Essentially, your customer cannot be forced into consent, or be unaware that they are consenting to processing of their personal data. They must also know exactly what they are consenting to and they must be informed in advance of their right to withdraw that consent. Obtaining consent requires a positive indication of agreement – it cannot be inferred from silence, pre-ticked boxes or inactivity. This means that informing the user during the opt in is becoming more important in the future.

The GDPR states that consent can be withdrawn at any time and it must be as easy to withdraw consent as it is to give it. For example, unsubscribing to marketing emails shouldn't be hidden behind a login screen.

The right to be forgotten

Individuals can demand that any data held on them is permanently deleted.

Data portability

GDPR makes it easier for users to request a copy of the data held on them in a common format.

What data can I collect?

GDPR doesn't prohibit the collection of data, it simply stipulates that:

- It should be clear what data is being collected
- Why the data is being collected
- What the data will be used for
- The user must actively opt-in to the collection and use of their data.

What do I do with my current data?

We recommend carrying out an audit of the current data you collect and store from your users. You should assess and document the personal data you hold currently, where it came from and who you share it with, how it is stored and whether it is still required.

You should also carry out an opt-in exercise of current subscribers. Unless you have documented active opt-in from your subscribers, contacting them with news or marketing materials after GDPR implementation will be non-compliant.

We recommend that you send out a communication to anybody currently held within your CRM or marketing list to invite them to actively opt-in to future communication.

This is an opportunity for you to get your value proposition across to your users. Whilst a proportion of those users will inevitably opt-out, those who opt-in have done so consciously and are more engaged with your brand as a result.

You should think about the format and content of this email and how you can use it as an opportunity to sell your brand and to tailor future communications to the recipient so they are more relevant in future. For example, you may wish to be granular in what types of communication the user wants to receive in future and the topic of such.

You may want to incentivise it, eg with a discount code or prize draw for those who opt in.

Does my cookie notice need to be updated

GDPR includes IP addresses as personal data and therefore any cookies which collect IP addresses require consent.

We recommend updating your cookie notice to include a yes / no option instead of the implied consent model currently in place on most websites.

As you may know, cookies are largely controlled at browser level so we suggest a user clicking 'no' to the cookie notice takes them to a page displaying instructions of how to disable cookies in the most popular browsers such as Google Chrome or Internet Explorer.

Does my Privacy Policy need to be updated?

Your Privacy Policy should include:

- Clear information about the identity of the organisation collecting the data.
- What information is collected.
- How the data will be used.
- Clear & straight forward information how to access personal information.
- Helpful privacy advice, for example, how to switch off cookies within a browser.

If your privacy policy does not include this information, you should update the content to ensure compliance.

Here is best practice advice from the Information Commissioner's Office regarding what should be included within a privacy notice:

https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf

Econsultancy have also published helpful advice around Privacy Notices:

https://www.econsultancy.com/blog/69256-gdpr-how-to-create-best-practice-privacy-notices-with-examples

What about the contact form on my website?

This represents the most visible change to websites from a GDPR perspective and almost all contact forms will require changes to be compliant.

Your contact form should include:

- A tick box - that is not pre-ticked - confirming the user understands your terms and conditions with hyperlinks to your terms & conditions and your privacy policy.
- A tick box - that is not pre-ticked – inviting the user to opt-in to future communications.
    - You may also want to specify how the user opts in to being contacted ie post, email, SMS etc
- The language should be clear and no confusing language or double negatives.

What are Innovation Digital doing about GDPR?

Here at ID we take data protection and privacy very seriously. Our processes are designed to ensure that your data is secure. We use only GDPR compliant suppliers such as our hosting provider, Iomart and have data processing agreements in place to ensure compliance throughout the supply chain.

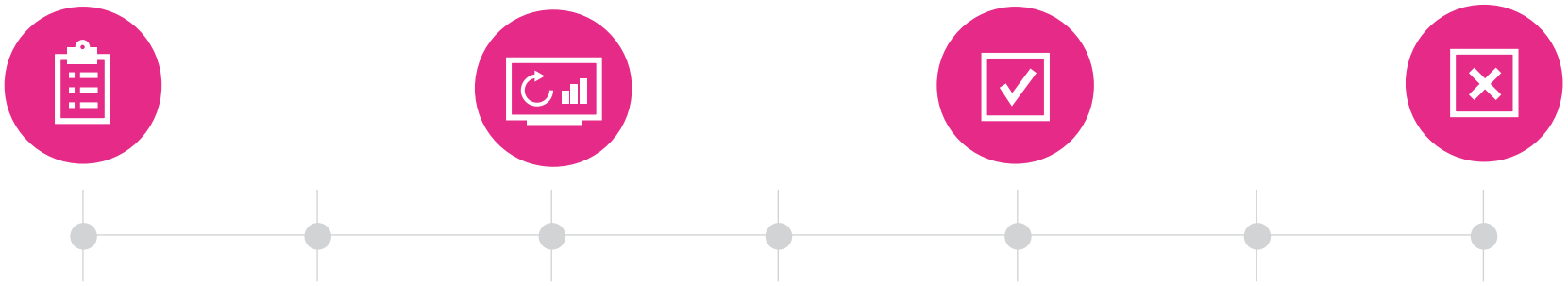
We can assist and facilitate the changes to your website to help you become compliant ahead of 25th May 2018.

Who can I speak to about GDPR?

We recommend that our clients seek their own legal advice about GDPR. However, your Account Manager is here to help you ensure your online presence is ready for the legislation coming into play. Feel free to get in touch with the team or our Data Privacy Officer, Lianne Dewar if you have any GDPR-related questions or queries.

The GDPR Checklist

We've put together this handy checklist to help you ensure your website and marketing activities are GDPR compliant.



1. Review your current data
2. Review your current data processing procedures
3. Obtain active opt-in from current subscribers
4. Ensure it is as easy to withdraw consent as it is to give it
5. Ensure your Cookie Notice is GDPR compliant
6. Ensure your Contact Form is GDPR compliant
7. Ensure your Privacy Policy is GDPR compliant