conscious

brand, design & marketing for law firms

General Data Protection Regulation (GDPR) – An Impact Assessment for Websites

Prepared by
Andrew Gray (Operations Director)

Version 3 – October 2017

Conscious Solutions Limited
Royal London Buildings
42-46 Baldwin Street, Bristol, BS1 1PN
Tel: 0117 325 0200
Email: sales@conscious.co.uk
Web: http://www.conscious.co.uk

Table of Contents

Version History

Date	Author	Notes
10-Jul-2017	David Gilroy	Review and finalising Version 1 for circulation to clients
30-Jun-2017	Andrew Gray	Initial draft for internal discussion
20-Oct-2017	Andrew Gray	Updated to be relevant to CMS-platform neutral

1 Introduction

The "General Data Protection Regulation" (GDPR) is new legislation that comes into effect in 25 May 2018. It replaces the Data Protection Directive (implemented as the Data Protection Act of 1998.

In this document we have provided a summary of GDPR and highlighted parts of the legislation that has an impact on the way that websites are built and operated – we have also tried to indicate some "grey areas" (open to interpretation) and made recommendations regarding "best practice". In other words, this document addresses GDPR with the narrow focus of "websites" - for a broader discussion about the impact of GDPR on law firms you might like to start with this article from the Law Society.

2 A Basic Guide to GDPR

2.1 Scope

- In essence the legislation is designed to protect citizens rights to privacy - to do this GDPR:
    - Specifies what is considered to be "personal data"
    - Regulates what can and can't be done with personal data
    - Regulates how personal data must be protected
    - Regulates the rights of citizens to access their data ("Subject Access Right")
    - Regulates the rights of citizens to have data removed ("Right to be Forgotten")
    - Regulates the rights of citizens to have inaccurate data corrected
    - Regulates the rights of citizens to obtain their data in a structured format ("Data Portability")

- GDPR applies to all organisations that handle or process data about EU citizens **regardless of location**. It applies just as much to Uber based in California as it does to BT based in London. The location of the organisation or the processing centre is no-longer relevant.

2.2 Types of Data

The legislation applies in different ways to different types of information:

- Personal Data
    - Any information that is linked back to an individual
    - Any information that **could be** linked back to an individual by some other organisation (even if you've not done the work to link it yourself)

    - It is not just data about a person's private life…. "personal information" can also be information about their public or professional life
    - Living individuals (GDPR does not apply to personal data about dead people)

- Sensitive Data
    - Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership;
    - Data concerning health or sex life and sexual orientation;
    - Genetic data or biometric data.
    - Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence).

2.3 Key Concepts

- **Privacy by Design** - is an approach to projects that promotes privacy and data protection compliance from the start (rather than them being bolted on as an after-thought or ignored altogether).

- **Privacy by Default** - simply means that the strictest privacy settings automatically apply once a customer acquires a new product or service. In other words, no manual change to the privacy settings should be required on the part of the user. There is also a temporal element to this principle, as personal information must by default only be kept for the amount of time necessary to provide the product or service.

- **Pseudonymous data** – the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information. Although GDPR recognizes that pseudonymization "can reduce risks to the data subjects," it does not mean that the data is unregulated: "personal data which have undergone pseudonymization, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person" (i.e., personal data). Thus, pseudonymization is "not intended to preclude any other measures of data protection"….. but use of pseudonymization reduces the risk and therefore makes a breach less likely to be notifiable.

- **Data Breach** - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

2.4 Primary Entities

GDPR places some specific responsibilities on "Data Processors", however, the vast majority of the responsibility is placed at the door of the "Data Controller". The fact that a Data Controller might decide to outsource certain functions to a Data Processor does not mean that the Data Controller is not still liable – they are liable even when the breach is the direct result of the Data Processor. The same entity can be a "Data Controller" in respect of some processing activities and a "Data Processor" in respect of other processing activities:

- Data Controller - the body which alone or jointly with others makes decisions about processing activities (regardless of whether it actually carries out any processing operations).
- Data Processor - the body which processes personal data on behalf of a Data Controller

2.5 Consent

The reasoning on this issue is that all individuals should know what data is being collected about them and why....and should have to give their consent.

- Information has to be freely given and consent must be unambiguous and explicit
- Requests for consent should be separate from other terms, and be in clear and plain language
- Individuals must have a real right to say no
- Data Controllers must be able to demonstrate consent (so have to keep records of how/when consent was given)
- Parental Consent is required if the individual is under 16 (13 in some EU countries)

2.6 Compliance

- The maximum fine per breach is €20m or 4% of global turnover (whichever is higher)
- GDPR is regulated in the UK by the Information Commissioners Office (ICO)
- You have to report breaches to the ICO (usually within 72 hours) but only if the breach "is likely to result in a risk to the rights and freedoms of individuals".
- You have to report breaches to individual subjects (usually within 72 hours) but only if the breach represents a "high risk" to their rights and freedoms

- Appointing someone as a “Data Protection Officer" is not a legal requirement but is expected for organisations with more than 250 people and doing so, even for smaller organisations, will help reduce the risk of prosecution

3 Impact on Website Design

3.1 Form Submissions is “Personal Data”

3.1.1 Current situation

The most obvious impact of GDPR on website design is that form submissions are almost always “personal data”. Typical examples include:

- General enquiry form
- Call-me-back form
- Conveyancing quotes
- Event registrations
- Wills questionnaires

This information is normally submitted to the website and then passed on to someone else via an email. However, the original data is usually stored indefinitely so that marketing and BD professionals can track trends in performance.

3.1.2 Modifications for GDPR Compliance

To be GDPR compliant without losing the benefit of being able to trend form-submission data the website builder would need to make the following changes:

- Form data should be separated into two parts which we can think of as “form-summary” and “form-detail”. Form-summary-data is high-level information about the form activity such as date/time, form title, channel, user’s email. Form-detail-data will be everything else (i.e. the contents of the form) which may often include personal data.
- Form-detail-data should only be held for 60 days
- Form-summary-data should be made anonymous after 60 days (i.e. email address will be removed)….. but it will be retained indefinitely so that marketing & BD can monitor long-term trends in performance.

Please note that the period of 60 days is not explicit in the GDPR legislation – it is our own judgement as to what can be defended as necessary and reasonable (“necessary” because enquiries transferred by email may get lost and need to be resent).

3.2 Newsletter Opt-in and Opt-out

3.2.1 Current situation

Forms that include an option inviting users to subscribe to a newsletter must default to "no" rather than "yes" – this has been best practice for a while and therefore something that is already implemented on most sites but nevertheless, worth checking.

GDPR is very clear that the process for opt-out has to be as easy as the opt-in process.

3.2.2 Modifications for GDPR Compliance

For GDPR compliance a you will need to audit your site to be confident about this issue. Most firms are using services like MailChimp and these already enforce easy opt-out processes.

Please note that there is no specific requirement to implement "double opt-in" (online registration followed by confirmation via an email link) but there is a requirement to be able to prove that the user agreed and to maintain an audit trail of their actions. A double opt-in process is well understood by users so is probably the best way to achieve this.

3.3 Online Payments

3.3.1 Current situation

Many websites include payment gateways that allow clients to pay invoices and send money on account. The technology behind these gateways varies significantly – some hand the payment transaction to a separate website while others integrate the payment experience into the website using an API.

3.3.2 Modifications for GDPR Compliance

Regardless of the technical solution used, the website may be collecting personal data such as name, address and invoice details before passing this information to the payment gateway. If that is the case the website will probably also be storing that information - you will need to modify the process to remove any personal data after 60 days (e.g. removal of email address and any other identifying information).

3.4 Registration

3.4.1 Current situation

Some sites invite users to register in order to use advanced features such as extranets. The registration process collects "personal data" including email address, username and password.

3.4.2 Modifications for GDPR Compliance

To be compliant the user must agree to Terms and Conditions that explicitly state what will happen with any personal information that you ask during the registration process. A double opt-in process is recommended.

You should also record the date of "last login" and flag as "inactive" accounts which have not been used for 12 months and any personal data associated with these accounts should be made anonymous (i.e. name and email address should be deleted).

3.5 Session Management

3.5.1 Current situation

Many websites give the user a session-cookie in order to distinguish the user from other users - however, the user remains anonymous at all times. This is done not because the website is trying to track individuals – it is necessary for the correct functioning of many features of the site, for example: the anti-spam CAPTCHA images presented on most forms. The system has to have some mechanism of knowing which CAPTCHA has been given to which user – the session-cookie provides this essential mechanism.

3.5.2 Modifications for GDPR Compliance

None – the session-cookie is not "personal data" because it can not be used to identify the individual.

3.6 Tracking by Third Party Software

3.6.1 Current situation

Some websites use third-party products such as CANDDi and Ruler Analytics. These products are used for the specific purpose of tracking users and alerting BD professionals when critical events happen (like a key-individual returning to the site…. or a specific person viewing your Terms & Conditions page).

At first glance you might expect the operation of these products to be against the spirit and the law of GDPR since they track users in ways that most users would not expect. However, the providers of these tools seem confident that they can still be GDPR-compliant.

3.6.2 Modifications for GDPR Compliance

There is risk associated with using third-party software. If that software does something that is illegal then under GDPR it is the responsibility of the Data Controller (you) not the Data Processor (them). For this reason it is important to study your contract with those organisations very carefully.

The contract between the Data Controller (i.e. the firm/owner of the website) and the Data Processer (i.e. the website agency/builder) needs to be explicit on this issue – the contract should identify any third-party software explicitly so that the Data Controller understands their responsibilities in that respect.

3.7 Google Analytics

3.7.1 Current situation

Almost all websites are configured to use Google Analytics for the analysis of usage data. The system has always been anonymous so we don't believe there is any "personal data" being collected.

3.7.2 Modifications for GDPR Compliance

None – we believe that use of Google Analytics falls outside the scope of GDPR.

3.8 Google Tag Manager

3.8.1 Current situation

Tag Manager is a product that enables a lot of powerful features – such as the ability to link in third-party software on particular pages. If Google Tag Manager is installed it becomes important to know who has access to it because those people have the ability to make drastic changes to your website.

3.8.2 Modifications for GDPR Compliance

The contract between the Data Controller (i.e. the firm/owner of the website) and the Data Processer (i.e. the website agency/builder) needs to be explicit on this issue – the contract should identify the people with access to Tag Manager explicitly so that the Data Controller understands their responsibilities in that respect.

3.9 Right to Access and Right to be Forgotten

3.9.1 Current situation

In some situations GDPR gives users the right to access the personal data that is held about them, and the right for this information to be corrected or deleted.

3.9.2 Modifications for GDPR Compliance

Any request for data access or removal can probably be processed manually by the website agency/developer - there is no legal requirement for the user to be able to do this themselves.

3.10 Privacy Notice

3.10.1 Current situation

Under existing legislation you are already required to give users certain information such as your identity and the purpose(s) for which you will process their data – information that is normally delivered via a Privacy Policy linked from the footer of most websites.

3.10.2 Modifications for GDPR Compliance

GDPR adds further requirements:

- the legal basis for processing the data (lawfulness of processing is set out in Article 6)
- the period for which personal data will be stored
- meaningful information about the logic involved, as well as the significance and consequences of such processing

This information must be provided in a concise, transparent, intelligible and easily accessible manner using clear and plain language. The ICO has published separate guidance on privacy notices under the GDPR.

Please note that to be compliant you will need to add information describing what you do with information once it has been passed to you from the website. For example, what happens to enquiry information once you receive it and how long is that information retained by your office systems (i.e. it's not only information about the website).

3.11 Terms and Conditions

3.11.1 Current situation

Your website will probably already include a legal statement presented as Terms and Conditions – this will need to be reviewed and modified as part of the GDPR effort.

3.11.2 Modifications for GDPR Compliance

Modify the statement to use the language of GDPR "data subjects", "data controller" and "data processor". The most important element as far as GDPR is concerned is to explain what personal data is collected and why. The legislation says that this information should be presented clearly and not buried amongst other legal terms so it's best to have a heading in your Terms & Conditions but then link through to a separate page for details (this page can also be linked to from forms and other parts of the site that collect personal information).

3.12 Contract with your Web Agency/Developer

3.12.1 Current situation

Most firms will already have a contract on place governing the relationship with their website agency/developer. However, these contracts probably don't use the language of GDPR and so may not be as clear as they need to be. For example: does the contract pass

3.12.2 Modifications for GDPR Compliance

We recommend reviewing the existing agreement to make sure that it uses GDPR terminology when specifying roles and responsibility ("Data Controller" vs. "Data Processor" etc.)