General Data Protection Regulation (GDPR) - A CANDDi perspective

1 - Summary

With General Data Protection Regulation less than 12 months away there is a legal requirement for all businesses to have taken the necessary steps for adherence.

Campaign and Digital Intelligence Limited as developers of the CANDDi software is no exception to this and is compliant.

2 - Introduction

The “General Data Protection Regulation” (GDPR), set to come into effect on May 2018, is European Legislation set to replace the 19 year old Data Protection Act (1998).

In this document we will seek to provide a summary of GDPR and discuss areas of compliance and opportunities presented as a result of the legislation. This will be discussed with specific focus on CANDDi*, the website analytics tool.

To use the CANDDi software there are certain requirements. However, once adopted CANDDi will be in a position to assist with broader legal obligations including, but not limited to; Subject Access Requests and Data cleansing.

**Nb. For the purpose of this document ‘CANDDi’ will be used in reference to the software and ‘Campaign and Digital Intelligence Limited’ for the Company.*

3 - Version History

Date	Author	Notes
11/10/2017	Edward Westbrook	Initial draft for discussion
13/10/2017	Edward Westbrook	Revised version for distribution approval
23/10/2017	Edward Westbrook	Revised version approved for limited release

4 - A Basic Guide to GDPR

GDPR is legislation written to protect EU citizens from privacy and data breaches in a world that is vastly different to when the Data Protection Act was established.

The legislation:

- Specifies what is “personal data”
- Regulates what can be done with “personal data”
- Define the roles and responsibilities of “controllers” and “processors”
- Answer the question of what is considered “consent”

5 - Technically, how does CANDDi work?

CANDDi is a website analytics and tracking tool. The software itself works by the Campaign and Digital Intelligence Client (herein the ‘Client’) placing a small snippet of Javascript code into the header/ footer of their website.

Once in place visitors to the website will be tracked using two first-party cookies. CANDDi is then able to associate website activity with a device linking sessions and visits.

CANDDi is able to link this device, and therefore onsite activity, with a visitor's identity and present this information within the CANDDi dashboard. There are 4 circumstances in which the visitor identity can be established, these are:

1. The completion of a website form
2. The completion of the CANDDi Capture
3. A visit to the website as a result of clicking through a tracked 1-2-1 email (in conjunction with CANDDi Outlook/ Gmail Plugin)
4. A visit to the website as a result of a bulk email marketing click-through

Where one of the above has **not** occurred the visitor's identity will remain anonymous.

CANDDi also monitors the IP address of the visitor. In some instances this will be registered/ linked with a company. In these instances CANDDi will display company level information until such time as one of the four ways in which to identify are fulfilled.

6 - GDPR, CANDDi and Cookies

Cookies are only mentioned once within GDPR. Recital 30 states:

"*Natural persons may be associated with online identifiers…such as internet protocol addresses, cookie identifiers or other identifiers…. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."*

In short, what this is stating is that when used to identify a device or, as with CANDDi, when used in conjunction with other data to identify the individual associated with that device it should be treated as personal data.

Personal Data is defined within the legislation in several ways:

- Any Information that is linked back to an individual
- Any information that could be linked back to an individual by another organisation (irrespective of who does this)
- Personal information can also include information about a person's public or professional life.

This raises 2 interesting areas for the lawful processing of personal data

1. Under Article 6(1)(a) - For the processing of personal data to be legal this must have the consent of the data subject, or;
2. Under Article 6(1)(f) - It must be "Necessary for the purposes of legitimate interests pursued by the controller..."

7 - GDPR, CANDDi, Cookies and *Article 6(1)(a)* Consent

Under GDPR the notion of 'consent' will also change for cookies that are not 'strictly necessary'. This is outlined in more detail within Recital 32:

*"Consent should be given by a **clear affirmative act** establishing a freely given, specific, informed and **unambiguous indication** of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or **conduct which clearly indicates in this context the data subject's acceptance** of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the **request must be clear, concise and not unnecessarily disruptive** to the use of the service for which it is provided."*

A shift towards a much more opt-in (or even soft opt-in) approach for cookies is therefore a likely position. This is not dissimilar to the current position under the EU Cookie Law.

There is however another condition on consent found in Article 7(3):

*"The data subject shall have the **right to withdraw his or her consent** at any time. …. It shall be as easy to withdraw as to give consent."*

When considered together it would be reasonable to conclude that consent will be valid if the website visitor is displayed an initial notice (and choice) and is able to change this, in a granular way, at a later date.

8 - GDPR, CANDDi, Cookies and Article 6(1)(f) Legitimate Interest

We can however extend this notion of consent to consider an alternative lawful ground for lawful processing of personal data. The setting of cookies based on the 'legitimate interests of the controller'. This would allow the use of cookies without the strict requirement of explicit consent as stated in Article 6(1)(a). *(nb. This would not apply to the public sector due to legislative distinctions)*

Article 6(4) sets out several conditions for the use of Legitimate Interest. A data controller would need to have considered their justification of such decision. Due to the way in which and what CANDDi tracks it is likely to fulfil such criteria. (Campaign and Digital Intelligence Limited cannot however advise on this as the justification is business specific.)

This is found in Article 6(1)(f) where there is lawful bases available for the processing of personal data where it is *"Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject"*

The recitals give examples of processing that could be necessary for the legitimate interest of a data controller including:

- Recital 47: "Processing for direct marketing purposes or preventing fraud"
- Recital 48: "Transmission of personal data within a group of undertakings for internal administrative purposes, including client and employee data"

Recital 47 would therefore cover the setting of first party cookies for marketing purposes.

Legitimate Interest does however also come with the right to object to the processing by the individual (Article 21). The website would therefore still be required to have the ability for the user to opt-out of such usage.

When considering how the Legitimate Interest approach would relate to the setting of cookies, and use of CANDDi, as a business development/ direct marketing tool this would appear to complement.

9 - CANDDi as a Data Processor

Article 4 of GDPR defines the different roles of the 'data controller' and 'data processor'. From a CANDDi perspective it is important to note that Campaign and Digital Intelligence Limited is a data processor.

No personal data is shared, or synced between client accounts. Any data processed is the property of the Client and remains as such.

Controller – "*means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*"

According to article 24 it is the responsibility of the controller to be able to demonstrate the processing is performed in accordance with the regulation.

Processor – "*means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*"

According to Article 28 from the EU GDPR, *processors should providing sufficient guarantees to meet the requirements of the Regulation and ensure the protection of the rights of the data subject.*

10 - Practical recommendations

To ensure compliance Campaign and Digital Intelligence Limited recommend review and consideration be taken to the below:

Cookie Banner - It is a requirement to inform the visitor to a website in a 'clear and unambiguous way' that Cookies are being used on the website. Under Article 6(1)(a) the existing generally accepted practice of continued browsing as "*conduct which clearly indicates in this context the data subject's acceptance"* will suffice as consent.

Cookie Statement - Should a complaince question or issue arise, additional scrutiny will be placed on contents of cookie policy/ statements. The existence of such policy, clearly explaining the description and purpose of the cookies used will assist in proving reasonable care has been taken to obtain freely given, specific and, most importantly, informed consent.

There are several services that provide functionality to satisfy the requirement found in Article 7(3). To assist specifically, with the right to withdraw consent.

Legitimate Interest - If using the legitimate interest principle within your website tracking it is advisable to have on record during your GDPR preparation that this is the case. This should include the grounds on which you are using this.

Glossary of Terms

- **Data Processor -** A *natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*
- **Data Controller -** *The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*
- **Personal Data -** Any information relating to an identified or identifiable natural person
- **First Party Cookies -** A small amount of text stored in the user's computer that is created by the website the user is visiting.
- **Third Party Cookies -** A cookie that is stored in the user's computer by a Web site from a domain other than the one a user is visiting
- **Bulk Email Marketing -** The sending of emails en masse, usually via an email marketing platform
- **CANDDi Capture -** A 'pop up' enquiry form, similar to an on-site contact us form
- **Cookie Policy -** The section of website detailing the types of cookies that are in use.
- **IP Address -** A numerical label assigned to each device connected to a computer network

Additional Sources:

- https://www.cookielaw.org/blog/2016/5/13/the-gdpr,-cookie-consent-and-customer-centric-privacy/
- https://www.econsultancy.com/blog/69303-gdpr-for-marketers-five-examples-of-legitimate-interests
- https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
- EU General Data Protection Regulation
- https://www.slaughterandmay.com/media/2535723/processing-of-personal-data-consent-and-legitimate-interests-under-the-gdpr.pdf