Coimisiún Cosanta Sonraí
Data Protection Commission

Discussion Paper – Regulation of Online Political Advertising in Ireland

Submission of the Data Protection Commission

2 November 2018

Introduction

The Data Protection Commission (the DPC) is the national independent authority in Ireland with responsibility for upholding the fundamental right of individuals to have their personal data protected, and enforcing the obligations of data controllers and processors in this context. The statutory powers, duties and functions of the DPC are detailed in the Data Protection Act 2018 (the 2018 Act) which gives further effect to the General Data Protection Regulation (EU) No. 2016/679 (the GDPR).

The DPC notes that the aim of the discussion paper is to "*outline the issues and challenges involved in regulating transparency of online political advertising and provide a basis for a public consultation in advance of an open policy forum to be convened in the autumn*". The DPC welcomes the opportunity to provide a submission in respect of what is a very important and timely subject matter and wishes to contribute to the regulation of online political advertising while operating within its legal framework and statutory remit. The DPC also wishes to provide some context and set out its current remit in respect of the regulation of the processing of personal data, and, in particular, the regulation of online political advertising including personal data relating to individuals' political views.

In this context, this submission seeks to provide an overview of the scope of the data protection law regime in Ireland including the necessity for a lawful basis to process personal data (such as consent) and the requirement for transparency in data processing. While the DPC considers the regulation of online political advertising is focused on specific goals (such as transparency in campaign funding) which differentiate it from the DPC's task to regulate the processing of personal data in broader terms, the DPC believes its perspective on the regulation of online political advertising may assist to inform the wider discussion on the prominent issues and challenges in relation to this matter.

Principles of Data Processing

"Personal data" is broadly defined and includes any information relating to an identified or identifiable living individual, which may be anything from a name, a photo, bank details, an email address, medical information and/or political opinions to a computer IP address. The DPC regulates the processing[1] of personal data (including political views of individuals) in both an online and offline context. The GDPR, the Act (which further gives effect to the GDPR at a national level) and Statutory Instrument SI 336/2011 *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* are some of the legislation which constitutes the DPC's legal framework for the regulation of data processing including the processing of personal data revealing political opinions.

At a minimum, the GDPR provides for certain overarching regulatory obligations which must be adhered to by relevant actors, i.e. "controllers" and "processors", which "process" or, in other words, handle, personal data in all its forms. The fundamental principles which should be adhered to when processing personal data and are set out in the GDPR[2] as follows:

- Personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject;
- Personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

[1] Processing is very broadly defined by the GDPR in Article 4(2) as '…*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*;".

[2] See Article 5(1) of the GDPR.

- Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These principles are central to the data protection regulatory regime and are similarly relevant to the processing of to personal data revealing political opinions (which is categorised as a "sensitive category of personal data"[3]) as well as processing personal data in the context of engagement of the electorate as part of the democratic process.

Lawful Basis

One of the most basic and important legal obligations to which controllers and processors are subject is to process personal data pursuant to a "lawful basis". A lawful basis may be, for example, an individual's consent, a contract or a legitimate interest of the data controller. In order to process personal data revealing political opinions, controllers may require an individual's explicit consent[4] to do so or another lawful basis provided for by law. Obtaining the explicit consent of an individual to the processing of personal data revealing political opinions can be an effective way of ensuring that an individual has complete control in respect of the way in which their personal data is processed because such explicit consent must at least be freely given, specific, informed and an unambiguous indication of the data by way of a clear affirmative action.[5]

As mentioned above, explicit consent is only one lawful basis which allows for the processing of personal data revealing political opinions. For example, section 40 of the Act provides for certain instances pursuant to which the sensitive categories of personal data may be processed by elected representatives in the context of the requests for representation. Separately, section 39 of the Act provides that personal data may be used by a member of either House of the Oireachtas, the European Parliament or a local authority or candidates for election[8] to communicate in writing with a data subject for electoral purposes. "Electoral purposes" is defined in the Act as including the dissemination

---

[3] "Special categories of personal data" is defined in Art. 9(1) of the GDPR as "..*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*…".
[4] Art. 9(2) GDPR.
[5] Art. 4(11) GDPR.
[8] Section 39(3) of the Act.

of information, including information as to a person's activities and policies, that might reasonably be of interest to electors.[9] However, while a legislative basis (or an alternative lawful basis) can meet the requirements of lawfulness of processing of personal data or sensitive categories of personal data under data protection law, such provisions do not guarantee that the other fundamental principles of data protection law are met.

Transparency – a Data Protection Law Perspective on Online Political Advertising

As detailed above, data protection law provides that personal data must be processed in a transparent manner. In a data protection law context, the concept of "transparency" has a specific meaning.[10] For instance, data protection law does not require that a political advertisement must be accompanied with information as to the *bona fides* of the advertisement nor does it provide that the identity of funder or financer of a political advertisement should be disclosed to individuals. Instead, the transparency provisions of the GDPR mandate that, for example, individuals be provided with information as to the purposes for which their personal data is processed and the existence of any data subject rights which may be available to them.

This is one of the reasons that the DPC considers that the requirements for transparency in a data protection law context do not take into the account the regulation of transparency of online political advertising specifically given that data protection law has a wider remit, namely the protection of personal data. This is supported by the fact that the degree of transparency required from a data protection perspective is generally not dependent on the type of data processing which is occurring, rather there are transparency provisions which apply to all types of processing of personal data by controllers whether that be the processing of political opinions, or any other personal data, which may be provided in either an offline or online context.

Online Political Micro-targeting

The DPC considers that one of the central issues for consideration when regulating online political targeting is the employment of online political micro-targeting. This practice was highlighted in particular by the developments involving Cambridge Analytica earlier this year. Political micro-targeting involves the processing of personal data to identify the political interests and preferences of

[9] See Section 39(4) of the DPA 2018.
[10] See generally the obligations in Article 12, 13 and 14 GDPR.

an individual (for example, in an online context, this may occur through the collection of information from an individual's online profile) and then to use this information to personalise that individual's online environment. The identification of the political interests and preferences may occur through monitoring the behaviour of an individual using online tools such as cookies, pixels, tags and beacons. However political micro-targeting may also occur in an offline environment.

A timely example of "offline" political micro-targeting is apparent from the recent decision of the UK's Information Commissioner's Office (ICO) involving "Emma's Diary". The ICO fined Lifecycle Marketing (Mother and Baby) Ltd, known as "Emma's Diary", £140,000 for illegally collecting and selling personal information of more than one million individuals.[11] Emma's Diary, which provides advice on pregnancy and childcare, sold the information to a third party data broker for use by the UK Labour Party. On foot of this, the data broker created a database which the Labour party used to profile new mothers in advance of the 2017 General Election. The ICO found that Emma's Diary's privacy policy did not detail that personal data would be used for political marketing or by political parties.

The DPC considers that data protection law plays a role to ensure that, any data processing which takes place in the context of political micro-targeting is fair and transparent. In practice this means that individuals are, at a minimum, aware as to what personal data is collected about them, how it is used and who it will be shared with so that individuals may control the processing of their personal data in a meaningful way. However, as stated above, data protection law does not mandate the provision of information which the DPC considers is crucial to fair and transparent online political advertising including the source of funding for an advertisement in either an online or offline context. The DPC considers that, given the specific focus of this regulatory activity, such activity sits with the wider regulation of the electoral system rather than with data protection authorities.

Risks of Online Political Advertising

There are a number of risks of which the DPC is aware when considering the practice of online political advertising. As outlined above in the ICO's recent decision in respect of Emma's Diary, appropriate transparency is likely to be a key factor to mitigate any risks which may arise. In this context, data protection law provides that any information in respect of the way in which information about the processing of an individual's personal data is presented must be in a "*concise, transparent, intelligible*

[11] For more information on this case please note the following link: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/08/emma-s-diary-fined-140-000-for-selling-personal-information-for-political-campaigning/

and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child".[12] In this sense, it is clear that transparency information which is provided in respect of the processing of children's personal data may be not appropriate for the processing of adults' personal data. This is also applicable to the processing of adults' or children's personal data in the context of the regulation of online political advertising. In addition, the risk of so-called "information fatigue" must be considered when evaluating the proposal for the effective regulation of online political advertising. Information fatigue could, for instance, give rise to an increase in user apathy online in relation to transparency information provided in respect of online political advertising.

The DPC also considers that, in particular, in an online environment, the risks posed by combining data sets in a political context i.e. the creation of so-called "big data", must also be considered. As mentioned above, data sets may be gathered by way of online tools such as cookies, pixels, tags and beacons, from third parties (including from data brokers), from the input of information by an individual as well as gathered from public and/or other accessible sources, including the electoral register.

Processing of personal data revealing political opinions and recent developments of the DPC

The regulation of the processing of personal data revealing political opinions and related activities is an area in respect of which the DPC has published a number of recent guidance documents. Most recently, the DPC published materials on data protection in the context of electoral and canvassing activities including guidance notes on "'Elections and Canvassing: Data Protection and Electronic Marketing'[13] and "Elections and Canvassing: Data Protection and Electronic Marketing – the Data Protection Rights of Individuals".[14] Earlier this year, the DPC also published guidance for users of online platforms to encourage them to use control settings that dictate the extent to which they are subject to behavioural advertising.[15]

---

[12] Article 12(1) GDPR
[13] https://www.dataprotection.ie/docimages/documents/Canvassing%20Elected%20Reps%20FINAL.pdf
[14] https://www.dataprotection.ie/docimages/documents/Canvassing%20-%20Individuals%20update%20final%20version.pdf
[15] https://dataprotection.ie/documents/PandAPrefs.pdf

In addition, the European Commission has published papers on the application of EU data protection law in the electoral context[16] and there have also been recent developments in respect of the agreed industry code of practice on online disinformation.[17] In this sense, the drawing up of an industry or statutory code of practice in respect of the regulation of political online advertising may be one way to allow for increased transparency and demonstrable accountability on behalf of all stakeholders.

Conclusion

Free and fair elections are imperative to the functioning of a democratic society and it is clear that meaningful transparency in online political advertising is central to these concepts. The DPC considers that this may require attention as a matter which is distinct to data protection law, given that data protection provides a broad regulation for the processing of personal data rather than specifically in respect of the regulation of online political advertising. The DPC considers that regulation is required in order to ensure that relevant actors behave in a way to facilitate free and fair elections and, in particular, the DPC considers there is merit to consideration of how best and most effectively regulate what it considers to be a central electoral issue inherent in online political advertising, namely transparency of campaign funding as well as other pertinent issues such as the use of "big data" in the context of online political advertising.

The DPC would like to thank the Department of an Taoiseach for inviting input on this issue and the DPC welcomes further engagement and looks forward to the outcomes of the Open Policy Forum.

[16] https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf
[17] http://europa.eu/rapid/press-release_STATEMENT-18-5914_en.htm