Ireland - Location data: are you compliant?

Published 1 August 2016

At the beginning of August, the Office of the Data Protection Commissioner ("ODPC") published guidance notes in relation to location data in order to assist both data subjects and data controllers in understanding their rights and obligations in relation to such data. This article will focus on the guidance as it relates to data controllers.

What is Location Data

Location data is any information about an individual's current location, or information about an individual's movements in the past. Such data is usually collected via electronic devices, such as smartphones or pedometers such as "fitbits", which contain sensors enabling the device to detect its own location. Similarly, tracing a company vehicle and data relating to the location of visitors to a company's website could constitute location data for the purposes of data protection legislation.

Location data can be analysed and used by the recipient of the data to target the data subject with targeted advertising and other targeted services.

Location data falls within the definition of personal data under the Data Protection Acts 1988-2003 (the "**DPA**") if: (i) the data relates to a living person and; (ii) it is possible to identify the person to whom it relates from the location data itself, or if it is possible to identify the person from the location data and any other information which the data controller is likely to acquire.

There are no set rules as to what location data will constitute personal data under the DPA and it will depend on each individual case and the context and range of data collected. In some cases, a broad indication of a location may be enough to accurately identify a person and therefore constitute personal data. The Article 29 Working Party published an opinion in 2011 which provides useful guidance in relation to the use of location data and what constitutes personal data for the purposes of the DPA.

What are Data Controller's obligations in relation to Location Data

Location data that falls within the definition of personal data requires the data controller to comply with all DPA legislative requirements.

For an overview of the obligations placed on data controllers, click here**.**

When Location Data is Sensitive Personal Data

Location data may be deemed sensitive personal data for the purposes of the DPA if sensitive information, such as the data subject's religious beliefs, political opinions or personal health can be gleaned from the location data gathered.

This could occur where location data might indicate to the data controller that the subject has been frequenting a particular place of worship, or specific political headquarters, or health centre. Therefore, data controllers need to be aware that they could unwittingly be collecting and processing sensitive personal data for the purposes of the DPA and must therefore be cognisant of the resulting obligations which arise under the DPA in relation to sensitive personal data. Further obligations are placed upon a data controller who processes sensitive personal data under the DPA.

The ODPC's guidance note on sensitive personal data provides a useful overview of these obligations and can be accessed here**.**

Consent under the DPA in relation to Location Data

Location data relates to the user of the device and not the owner. This is an important consideration for the data controller as they must ensure they obtain consent from the user (and not the owner of the device) to process his or her data.

In their 2011 guidance, the Article 29 Working Party indicated that consent cannot be given by a data subject as part of the general terms and conditions of a service and that the subject's specific attention must be drawn to the fact that location data will be processed. Finally, the data subject must be given the option to opt out of the processing of his or her location data.

Recommended Next Steps

It is crucial that data controllers who are dealing with location data ascertain whether such data is personal data or sensitive personal data for the purposes of the DPA.

Data controllers should:

- identify any location data they are processing and whether it might constitute personal data or sensitive personal data;
- identify what the processing is meant to achieve;
- identify the minimum information required to achieve that purpose;
- identify any risks which the location data processing may pose;
- delete any location data which is no longer needed or being used;
- keep in mind at all times the data protection legislative requirements, in particular the DPA; and
- implement a location data protection policy detailing the requirements placed on data controllers pursuant to data protection legislation, which must be followed by all individuals dealing with location data within the company.

Organisations should ensure that any use that they make of location data is compliant with the ODPC's new guidance notes.

To see the ODPC's two guidance notes on location data, click here for guidance for data controllers and here for guidance for data subjects.

A press release from the ODPC on the new guidance notes can be accessed here.

Authors

Rowena McCormack
Dublin
rmccormack@dacbeachcroft.com

DAC BEACHCROFT