Personal data — an expanding concept?

Davinia Brennan, Associate at A&L Goodbody,

examines the definition of personal data in light of the recent ruling of the European Court in Breyer, the Irish Data Protection Commissioner's Guidance, and the incoming GDPR

Despite it being essential to understand whether information is 'personal data' in order to determine whether or not data protection law applies, much uncertainty surrounds the scope of the concept.

And whilst the now quite old Article 29 Working Party Opinion 4/2007 (copy at: www.pdp.ie/docs/1030) provides some guidance on the concept, uncertainty prevails — particularly in regard to whether online identifiers, such as IP addresses and cookies, and pseudonymous data, such as key-coded data, constitute 'personal data'.

The decision of the Court of Justice of the European Union ('CJEU') in *Breyer v Bundersrepublik Deutschland* (Case C-582/14), (www.pdp.ie/docs/1031) along with recent guidance launched by the Irish Data Protection Commissioner ('DPC') on pseudonymous and anonymous data (www.pdp.ie/docs/1032), provide some welcome clarity on the concept.

This article considers the effect of guidance and cases in expanding the definition of personal data under the Data Protection Directive (95/46/EC), as well as how the definition will change under the General Data Protection Regulation, coming into force in May 2018.

The current definition of personal data

The Data Protection Directive (95/46/EC) defines 'personal data' as 'any information relating to an identified or identifiable living individual'. It provides that an identifiable person is 'one who can be identified directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

The Data Protection Acts 1988 & 2003 ('the DPAs') define personal data in a similarly broad manner as 'data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller'.

A person's name may be 'personal data', where it directly identifies that individual. A person may also be indirectly identifiable by their car registration number, social security number or a combination of criteria such as age, occupation, and place of residence.

Whilst the concept appears relatively straightforward, its interpretation has proved difficult in practice. For example, a common name may not be sufficient to identify someone from the whole of a country's population, but it may be sufficient to identify them in their workplace. Therefore, the extent to which certain identifiers are sufficient to achieve identification is very much dependent on the context of a particular situation.

Opinion 4/2007 of the Article 29 Working Party ('the Opinion') helpfully broke the definition of 'personal data' down into four component parts:

- 'any information';
- 'relating to';
- 'an identified or identifiable'; and
- 'natural person'.

The Opinion considers that these elements together determine whether a piece of information should be considered 'personal data'.

The first element, 'any information', calls for a wide interpretation, and includes objective and subjective information, such as statements and opinions about a person, whether true or false, and irrespective of the technical medium on which it is contained.

As regards the second element, information can be considered to 'relate' to an individual when it is 'about' that individual.

The third element requires that the information relate to a natural person that is 'identified or identifiable'. The Working Party considers that a person is identifiable when, although the person has not been identified yet, it is 'possible' to do so.

The question of when a person is 'identifiable' has proved to be a particularly difficult one, and we will focus on this element for the purposes of this article.

Finally, the fourth element requires the personal data to be about a 'living individual'.

When is a person 'identifiable'?

The Directive contains a broad test for determining whether an individual is 'identifiable'.

Recital 26 provides that account should be taken of 'all the means likely reasonably to be used either by the controller or by any other person to identify the said person'. Therefore to determine whether a person is 'identifiable', you must examine what means and available datasets might be used to identify a data subject. The Working Party considers that a mere hypothetical possibility to single out an individual is not enough to consider the person as identifiable if that possibility is negligible. It suggests that the criterion, 'all the means likely reasonably to be used', to identify a person, requires a range of factors to be taken into account, such as the cost of conducting identification, the purpose and advantage pursued by the controller in the data processing. The Working Party highlights that 'to argue that individuals are not identifiable where the purpose of the processing is precisely to identify them, would be a sheer contradiction in terms'.

"It would be wise for organisations not to view Principle 14(g) of the Shield as providing a 'carte blanche' for transferring key-coded data for pharmaceutical research purposes, where there is a legal means by which the data can be re-identified to an individual."

Are IP addresses identifiable personal data?

The status of IP addresses has caused much controversy. The Working Party discussed the processing of IP addresses by copyright owners at example 15 of its Opinion. It notes that where such processing is carried out by copyright owners for the purpose of identifying and prosecuting copyright infringers, the copyright owner anticipates that the 'means likely reasonably to be used' to identify the persons will be available, such as through the courts appealed to, 'otherwise the collection of the information makes no sense'. Therefore, the Working Party considers that IP information should be treated as 'personal data'.

The Working Party further looked at the scenario where an IP address does not allow identification of the user, such as where an IP address is attributed to a computer in an internet café, where no identification of the customers is requested. It pointed out that the ISP will probably not know whether the IP address in question is one allowing identification or not, and so the ISP 'will have to treat all IP information as personal data, to be on the safe side'.

Despite the Opinion, the Irish courts adopted a narrow construction of the concept of 'personal data' in *EMI Records (Ireland) Limited v Eircom Limited* [2010] IEHC 108, ruling that IP addresses were 'personal data' in the hands of an ISP, but not in the hands of record companies.

The decision in *Breyer*

The decision referred to in the introduction, *Breyer,* has been lauded as clarifying that a dynamic IP address may be 'personal data' in the hands of a person, such a website provider, even though additional information has to be sought from a third party ISP to identify the data subject. The CJEU held that the key question in determining whether information is 'personal data', is whether there is a legal means, reasonably likely to be used, to identify the person to whom the data belongs.

In determining whether those means are likely to be used, the court will take into consideration the effort involved, in terms of time, cost and manpower. Accordingly, whether information is 'personal data' must be determined on a case-by-case basis.

The decision is in line with the Opinion, but is at odds with the approach taken by the Irish courts in *Eircom* insofar as it confirms that all of the information enabling identification of the data subject does not need to be in the hands of one person.

IP addresses are also likely to considered 'personal data' under the GDPR. The Regulation defines 'personal data' as including information such as 'an online identifier' where it can lead to identification of individuals, when combined with other information. Recital 30 comments that online identifiers, such as an IP addresses and cookies, '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 individuals and identify them'.

Is pseudonymous data personal data?

Pseudonymisation is a method of replacing one attribute in a record, such as a name, with another, such as a unique number. An individual is therefore still likely to be identified indirectly.

Although the *Breyer* decision does not expressly refer to pseudonymous data, it is recognised as supporting the view that pseudonymous data may be 'personal data' and fall within the scope of the Directive, where there is a legal means by which the data can be retraced to an individual, which does not involve disproportionate effort in terms of time, costs and manpower. Due to the risk of re-identification, even where tech-

(Continued on page 6)

(Continued from page 5)

nical and organisational measures are in place, it would be prudent for organisations to treat all pseudonymised data as 'personal data'.

This approach is consistent with the view of the Working Party in the Opinion and also in Opinion 5/2014 on Anonymisation techniques (copy at www.pdp.ie/docs/1033), as well as the approach taken by the DPC in her guidance published earlier this year ('the Guidance'). In the Guidance, the DPC warned that while pseudonymisation is a useful security measure, it is not a method of anonymisation, and pseudonymised data remains 'personal data'.

The Working Party and the DPC do not regard irreversibly anonymised data as constituting 'personal data'. However, the threshold for truly anonymised data is extremely high.

The DPC notes that if an organisation does not delete source data at the time that anonymised data are prepared, the anonymised data will still be considered 'personal data' and subject to data protection law. In assessing what level of anonymisation is necessary, the DPC suggests that organisations should consider which methods are 'reasonably likely' to be used by an intruder, or by someone inside the organisation, to identify an individual. In making such determinations, organisations should have regard to the current state of technology and the information that is available for re-identification purposes.

Pseudonymous data and the Privacy Shield

Interestingly, the issue of key-coded data in relation to pharmaceutical research was addressed in the European Commission's FAQs to the Safe Harbor framework, and in Principle 14 (g) of the Privacy Shield replacing that framework.

Both indicate that key-coded data, transferred from the EU to the US for pharmaceutical research purposes, does not constitute a transfer of 'personal data' that would be subject to the Principles. In its Opinion, the Working Party considered the Safe Harbor FAQs not inconsistent with its view that key-coded data are 'personal data' for all parties that might be involved in the possible identification of an individual. The Working Party arrived at its conclusion on the basis that the recipient in the US (i.e. the pharmaceutical company) receives only the key-coded data and will never be aware of the identity of the patients, which is known only to the medical professional/researcher in the EU.

The Working Party's take on the issue may need to be reconsidered in light of the broad construction of personal data taken by the CJEU in *Breyer,* and the GDPR coming into force. Accordingly, it would be wise for organisations not to view Principle 14(g) of the Shield as providing a 'carte blanche' for transferring key-coded data for pharmaceutical research purposes, where there is a legal means by which the data can be re-identified to an individual. Instead, organisations would be best treating such key-coded data as 'personal data' within the remit of EU data protection law, and subject to the Shield's principles, where appropriate.

Pseudonymous data under the GDPR

Unlike the Directive, the GDPR explicitly recognises the concept of pseudonymisation.

The GDPR also encourages pseudonymisation of personal data as a privacy-enhancing technique. Recital 28 of the GDPR provides that pseudonymisation 'can reduce the risks to the data subjects' and 'help controllers and processors to meet their data-protection obligations'.

However, pseudonymised data remain subject to the remit of EU data protection law where they can lead to the identification of an individual. Recital 26 states that 'personal data which have undergone pseudonymisation, 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').

Is the concept of personal data broader under the GDPR?

The GDPR, like the Directive, defines personal data as 'any information relating to an identified or identifiable natural person'. However, it specifies some new identifiers, including 'location data' and 'online identifiers'. Although location data and online identifiers are not expressly included in the definition in the Directive, it is clear from both Article 29 Working Party guidance and DPC guidance that they are both regarded as a means of indirectly identifying individuals. Accordingly, the GDPR should not be a 'game-changer' in this respect for those organisations that have been following such guidance.

Conclusion

In light of the decision in *Breyer* and the 'new' categories of personal data in the GDPR, along with the hefty fines for non-compliance, it would be prudent for organisations to take steps now to review the data that they collect, and assess whether such data fall within the definition of 'personal data' in the GDPR. The express inclusion of location data and online identifiers in particular will affect network providers, app developers, device manufacturers, and those involved in data analytics, behavioural advertising and social media. Such organisations will therefore need to amend their policies and procedures to ensure compliance with the new rules.

Davinia Brennan
A&L Goodbody
dbrennan@algoodbody.com