Sensitive personal data — current and future

Ann Bevitt, Partner at Cooley (UK) LLP, reviews the current position regarding 'sensitive personal data', including the requirements for processing such data, as set out in the EU Data Protection Directive, UK data protection law, the ICO's guidance, the Article 29 Working Party's Advice Paper, relevant EU case law, and the changes to be introduced in the Data Protection Regulation

Ann Bevitt is leading a session on 'Implementing the Lessons Learned from Recent Data Breaches' at the 14th Annual Data Protection Compliance Conference, being held in London on 15th and 16th October 2015. Details about this and all the other available Workshops are now online: www.pdpconferences.com/workshops

In the UK, Section 2 of the Data Protection Act 1998 defines sensitive personal data as personal data consisting of information as to the racial or ethnic origin of a data subject; his political opinions; his religious beliefs or other beliefs of a similar nature; whether he is a member of a trade union; his physical or mental health or condition; his sexual life; the commission or alleged commission by him of any offence; or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

According to the UK regulator's Guide to Data Protection (copy available at www.pdpjournals.com/docs/88416) 'the presumption is that because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data'.

Although this justification for increased consideration may be reasonable for the majority of the types of sensitive personal data listed above (although one queries whether trade union membership s in reality particularly sensitive), it is not easy to see why other types of information, such as financial data (for example, credit card and bank account details) should not also qualify for enhanced protection.

The Information Commissioner's Office ('ICO') recognises that there are gradations of sensitivity: details about a data subject's mental health, for example, are clearly much more sensitive than information regarding a broken leg, which may be obvious to anyone who sees the data subject. The ICO also notes that the same information may be both sensitive and non-sensitive personal data, depending on how they are processed. For example, although religion or ethnicity may often be inferred from a data subject's name, the ICO takes the view that:

'it would be absurd to treat all such names as sensitive personal data… Nevertheless, if [a data controller] processed such names specifically because they indicated ethnicity or religion, for example to send marketing materials for products and services targeted at individuals of that ethnicity or religion, then [the data controller] would be processing sensitive personal data'.

What are sensitive personal data — the current position in the EU

Article 8 of the Data Protection Directive (95/46/EC) sets out the conclusive list of categories of sensitive personal data, which is reflected in the list in Section 2 of the DPA set out above. In some Member States, local implementing legislation has included additional categories of sensitive personal data. For example, some Member States include genetic data and biometric data, and data relating to addictions.

The Article 29 Working Party's Advice Paper (copy available at: www.pdpjournals.com/docs/88417) recognises the difficulties in having a list of categories of sensitive personal data. Like the ICO's Guide, the Advice Paper recognises that there are degrees of sensitivity; for example, health data may range from the highly sensitive, such as information about a disability, to the completely non-sensitive, such as information about a cold or cough.

The Advice Paper also notes that photographs can reveal information about a person's ethnic origin or health, and therefore may be considered sensitive personal data. More fundamentally, the Advice Paper also questions whether a conclusive list is the correct approach in light of the rapid scientific and technological developments which can readily create new, and potentially very sensitive (in the non-technical sense), forms of data. If there is to be a list, however, the Advice Paper proposes that genetic data should be included, and possibly also biometric data, data relating to minors, financial information and geo-location data.

UK and EU requirements for processing sensitive personal data

Having established what is (or what may be) personal data, what are the enhanced protections regarding its processing?

In summary, as well as satisfying one of

the general conditions for processing personal data set out in Schedule 2 of the DPA, when processing sensitive personal data, a data controller must also satisfy a Schedule 3 condition. The Schedule 3 conditions most commonly relied upon are: the data subject has given his explicit consent; the processing is necessary to comply with employment law; the data subject has deliberately made the information public; the processing is necessary in relation to legal proceedings, for obtaining legal advice, or otherwise for establishing, exercising or defending legal rights; and where the data relate to racial or ethnic origin, the processing is necessary for monitoring equality of opportunity and is carried out with appropriate safeguards for the rights of data subjects.

The requirement that consent be explicit indicates that the data subject's consent cannot be implied. Rather, it must be absolutely clear and should cover the specific processing details such as the type of sensitive personal data (or even the specific information itself) to be processed, the purposes of the processing, and any special aspects of the processing that may affect the data subject, for example, any disclosures of the data that may be made.

UK and EU case law

There are only a handful of decided cases which deal with the processing of sensitive personal data. An early EU case illustrating how easy it can be to get things wrong is that of Ms Bodil Lindqvist, who got into trouble for writing about individuals on her home page without their prior consent. Ms Lindqvist's reporting of one individual having injured her foot and as a result working part-time was held to be sensitive personal data, and Ms Lindqvist was subject to criminal prosecution in Sweden as a result.

AB v. A Chief Constable is an interesting UK case from 2014 dealing with the disclosure of sensitive personal data (in this case, sick leave information) in the context of a reference. AB, a police officer, was charged with gross misconduct and subsequently took sick leave. Whilst on leave, AB asked for a standard reference to be sent to a prospective new employer. It was the police force's policy to provide basic information only, which would not include details of either AB's absence or the allegations against him. However, on this occasion, having provided a basic reference, the force then sent a second reference which contained information about both AB's absence and the disciplinary proceedings. The High Court found that the police had unlawfully disclosed AB's illness record, which constituted sensitive personal data, as no Schedule 3 condition had been met.

Most recently, Google's covert Safari browser tracking has also been challenged in the courts on the basis that Google obtained and collated internet users' browser-generated personal data and sensitive personal data, such as racial origin, political affiliations and religious beliefs without their knowledge or consent.

Google's appeal against the order allowing the claimants to serve proceedings on Google in the US was rejected by the UK's Court of Appeal at the end of March 2015. The Court held that there was a serious issue to be tried as to whether the browser-generated information was, in part, sensitive personal data.

Looking ahead: the draft Regulation

The current draft of the Data Protection Regulation refers to 'special categories of data' rather than sensitive personal data (see Article 9). Interestingly, in light of the recommendations of the Working Party in the Advice Paper, the categories of such data have been widened to include genetic data. During the discussions about and negotiations over the text of the Regulation, various proposals were made to increase further the special categories of data expressly to include gender identity, trade union activities (as well as trade union membership), biometric data and administrative sanctions. However, these have not been adopted.

The conditions for processing these special categories of data have also increased; for example, the conditions for processing health data have expanded (see Article 81) and these special categories of data may also be processed where necessary for the purposes of historical, statistical or scientific research purposes (which reflects the wording in Recital 34 of the Directive), subject to the safeguards set out in Article 83. This increase in the available grounds for processing special categories of data has worried some commentators who view it as a weakening of the protections for this type of data.

Interestingly, the draft Regulation takes a much firmer stance than the current Directive in relation to automated processing; under Article 20, profiling using the special categories of data will not be allowed unless explicit consent is given, or the profiling is in the public interest, and in both cases the individual's legitimate interests much be safeguarded.

The draft Regulation also imposes a new obligation on both data controllers and data processors to conduct an impact assessment before undertaking processing that presents a specific privacy risk by virtue of its nature, scope and purposes (see Article 33).

Article 33(2) sets out a non-exhaustive list of categories of processing that will fall within this provision, which includes the analysis of data on sensitive subjects, such as sex life or health, and the mass processing of genetic or biometric data.

Conclusion

The processing of sensitive data requires sensitive handling. The draft Regulation acknowledges this and, in some areas, extends the protections afforded to such data. However, the draft Regulation does not address all of the criticisms that have been made of the current sensitive personal data regime, and to that extent could be seen as somewhat of a lost opportunity for enhancing the safeguards for such data.

Ann Bevitt
Cooley (UK) LLP
abevitt@cooley.com