Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 14, NUMBER 9 >>> SEPTEMBER 2014

The U.K. Information Commissioner's Office Report on 'Big Data' and Data Protection

By Emma L. Flett and Ben Robson, of Kirkland & Ellis International LLP, London.

The Rise of 'Big Data'

The past few years have seen significant advances in the production and availability of high-capacity analytical information technology solutions. Those solutions provide the tools with which businesses, both big and small, are able to capture, translate and utilise high-value, high-velocity and high-variety information — so-called "big data".

In business terms, big data enables organisations to better understand their processes and customers. It can be used as a tool for measuring, predicting, planning and improving. In many respects, it is transforming the way in which businesses think. In legal terms, big data presents big questions, including how organisations that collect and process such vast amounts of information ensure that they do so within the framework of legal and regulatory restrictions.

Big Data and the Law

On July 28, 2014, the U.K. Information Commissioner's Office (the "ICO") published its report "Big data and data protection" (the "Report"). The ICO was keen to explore the legal issues raised by big data and, in particular, how the processing of personal data in this new landscape impacts the data protection principles in the U.K. Data Protection Act 1998 (the "DPA") and the proposed EU General Data Protection Regulation (the "Regulation") to replace the EU Data Protection Directive (95/46/EC) (*see analysis at WDPR, February 2012, page 4*).

The Report was compiled following one year's research, between June 2013 and June 2014, during which time the ICO analysed various reports and articles, conducted practitioner interviews and discussed the topic with experts at conferences and seminars. However, big data is a fast-evolving phenomenon, and, whilst the resulting Report is comprehensive, the ICO readily admits it is "subject to improvements and amendments in the future".

The Report recognises that not all instances of big data analytics involve the processing of personal data. It uses the examples of climate and weather data, which can be collected and used to enable new discoveries and improved services, and data collected from GPS-enabled buses to report arrival times to passengers. The collection and processing of such data does not fall within the scope of the DPA or the Report. Rather, the ICO's principal concern is where organisations collect and process data which is either entirely, or in some part contains, personal data. In these circum-

stances, the ICO notes that such organisations "must ensure they are complying with their obligations under the DPA".

It is clear that the ICO considers the current legal and regulatory landscape as being fit for purpose in the age of big data.

In 2012, the ICO published guidance ("Determining what is personal data") on the definition of "personal data", which, broadly speaking, is data which relates to an identifiable living individual. The "identifiable" element means that either the data *per se* enables the individual to be identified, or the data combined with other information can enable the individual to be identified. In its Report, the ICO refers to certain examples of personal data which may feature in big data analytics. These include data from monitoring devices which are used on patients in clinical trials, mobile phone location data, data on purchases made with loyalty cards and biometric data from devices worn on the body.

The Report focusses on three key legal considerations in the context of processing personal data as part of big data analytics:

- the need for a data processor to adhere to the first principle of the DPA (namely, fairness and lawfulness);
- the need for a data processor to be clear with data subjects about the purpose for which their data will be processed; and
- the need for processing of personal data to be aligned with the DPA's concept of "data minimisation".

The Condition of Fairness and Lawfulness

The Report notes that personal data must always be processed in accordance with the first data protection principle of the DPA, namely, fairness and lawfulness. Fairness, the ICO says, should be any organisation's first consideration in the context of big data analytics.

To ensure that the processing of personal data is fair, data processors need to be transparent with data subjects and consider the effect of such processing on those data subjects. The Report highlights the well-publicised example of the Target retail chain in the U.S., which used a complex algorithm to determine the due date of a woman's baby based on the dates of certain purchases from its stores. On the basis of this algorithm, a female high school student received coupons for pregnancy and baby products which Target deemed were appropriate to the stage of her pregnancy. The student's father complained to Target on the basis of her age and the fact that she was not pregnant, only to subsequently find out that she was. The Report notes that the U.S. has a different data protection regime to the U.K.'s, but nevertheless uses the example for the purposes of explaining when issues of fairness and customer expectations can arise in the context of big data.

The Report also notes the following in relation to fairness, transparency and privacy:

- The concept of transparency, which is incorporated into the DPA in the form of a "fair processing notice", needs to be promoted by organisations at an early stage, *i.e.*, at the point of collection;
- If data is processed for the purpose of making decisions about an individual (such as calculating his or her insurance premium) rather than merely contributing to research, then "the assessment of fairness must be even more rigorous"; and
- If the processing of an individual's data could result in profiling, for example, assessing creditworthiness based on a person's location, spending habits or contacts, care must be taken not to perpetuate stereotypes or bias — particularly where the decision is based solely on an automated process.

Not only must the processing of personal data be fair and transparent, but it must also meet further conditions set out in the DPA. Of these, the most relevant in the big data context are:

- consent;
- whether processing is necessary for the performance of a contract; and
- the legitimate interests of the data controller or other parties.

With regards to consent, the ICO makes clear in the Report that the "complexity of big data analytics should not become an excuse for failing to seek consent where it is required". Organisations should instead select an appropriate moment at which to notify data subjects of the purpose for which their data will be used, and respect the data subject's specific consent (or lack thereof) when processing data.

Processing of personal data does not always require consent. There is an exception to the consent requirement if it is necessary to process personal data where the data subject is party to a contract. As the Report points out, in the context of big data, not all of the subject's personal data may be strictly "necessary" for the processor to carry out a particular function. The ICO uses the example of data subjects who supply credit card details, names and addresses in order to complete online purchases. If other personal data is processed, it may not be strictly necessary to complete the purchase. However, if online payment methods were to adapt in future, then processors may be able to rely on this condition of necessity to complete a data subject's transaction.

More complex still is the alternative condition, that the data should be processed in the legitimate interest of the data controller or third parties. Those interests may include market research or ensuring the security of the subject's data or the controller's information technology systems. The processing for such a purpose again needs

   ISSN 1473-3579

to be necessary, and not merely desirable, for the data controller. The interests of the data subject need to be balanced against the controller's legitimate interests, using what the Report calls "a complex assessment involving a number of factors". Where big data is concerned, there is perhaps an argument to be made that the collection of vast amounts of personal data requires even greater deference to the data subject's privacy, though, as always, this balance has to be struck on a case-by-case basis.

The Purpose Limitation

Processing personal data is often carried out with a specific purpose in mind, such as determining the health of, or a treatment plan for, a patient, or allowing companies to see what their customers are buying in order to track stock levels or trends. However, high-value, high-velocity and high-variety information means that organisations could use the data for any number of different purposes, sometimes outside the scope for which that organisation has received the data subject's consent. This "repurposing" of data is something which the ICO is particularly keen to ensure takes place within the framework of the DPA.

The second data protection principle under the DPA, the purpose limitation, creates a two-part test:

- first, the purpose for which the data is collected must be specified and lawful; and
- second, if the data is further processed for any other purpose, it must not be incompatible with the original purpose.

One of the key benefits to collecting vast amounts of data is the way in which it enables organisations to realise almost endless (and perhaps initially unpredicted) purposes for which to use that data.

But is this benefit at odds with the purpose limitation?

The ICO considers that it might not be. The Report talks about the purpose limitation as being something more akin to a "non-incompatibility" limitation. It refers to the EU Article 29 Data Protection Working Party's April 2013 opinion on purpose limitation[1] , which refers to "functional separation" as a means of setting safeguards for dealing with big data (*see analysis at WDPR, May 2013, page 4*). So, for example, data which is initially processed for statistical purposes or other research purposes should not be available to support measures or decisions that are taken with regard to the individual data subjects concerned (unless specifically authorised by those data subjects).

The ICO considers that the question of compatibility can be assessed by reference to fairness. It cites the following example: "If information that people have put on social media is going to be used to assess their health risks or their credit worthiness, or to market certain products to them, then unless they are informed of this and asked to give their consent, it is unlikely to be either fair or compatible".

Data Minimisation

It is not just the issue of purpose limitation which appears to sit at odds with big data. The DPA also refers to the concept of "data minimisation" in two of its key principles: first, that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed, and second, that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. Big data, by contrast, is concerned with the collection of vast quantities of data.

However, the Report states that data minimisation need not be at odds with big data analytics. So long as organisations are able to articulate at the outset why they need to collect and process particular datasets, the collection of big data may be perfectly "adequate, relevant and not excessive" in relation to that objective. However, organisations should not leave it until after the collection and processing of personal data to determine whether it has been an "adequate, relevant and not excessive" exercise.

"Big data is not a game that is played by different rules".

ICO Report

With regards to data retention, again the ICO states that big data need not mean excessive retention. In fact, from the research conducted as part of the background to the Report, the ICO did not find any evidence of organisations changing their existing data retention periods solely on the basis that big data analytics were being utilised. The ICO states that, if organisations wish to retain big data for longer than is necessary, they should have considered the reasons for doing so, which can be articulated to the data subjects in question.

Anonymisation

The data protection principles in the DPA apply only to personal data and not to fully anonymised data. Therefore, anonymisation can be a tool to help organisations to carry out innovative analytics or storage.

The Report notes that some examples of big data analytics require only anonymised data, such as Telefónica's Smart Steps tool[2] , which tracks crowd movements based on mobile phones linked to its network, or during clinical trials to ensure that patient details are stripped out before the remaining data is used for research purposes.

However, it is important to note that organisations which anonymise data before using it for a particular purpose must take steps to reduce the risk of re-identification. Those steps must be proportionate to the risk. In November 2012, the ICO published an anonymisation code of practice which provides guidance on data anonymisation[3] .

Notably, the ICO points out in its Report that anonymisation should not be seen as a way to bypass the regulatory burden of the DPA on data processors. Rather, it

should be seen as a tool to prevent and mitigate the effects of data and security breaches. As data processors gather more and more information on data subjects, the risk of such breaches and their effects increase considerably. Depending on the nature of the organisation and the use or uses to which it intends to put big data, anonymisation therefore could be a tool worth considering from a risk management perspective.

Big Data and the EU Regulation

The Regulation is in draft form and does not currently have legal effect in the EU. Nevertheless, the ICO indicates that certain of its provisions are likely to affect big data analytics. The ICO published a separate detailed report in February 2013 on the likely impact of the proposed Regulation[4] (*see analysis at WDPR, March 2013, page 13*).

With regards to the impact of the EU Regulation on big data in particular, the Report notes that its provisions are likely to cover the following points:

- data minimisation and anonymised data;
- an onus on data controllers to justify the processing;
- the need for transparency;
- building in data protection by design and default;
- a shift in the balance of power; and
- a possible extension of data protection duties to organisations outside the EU.

The Regulation also suggests "a desire to shift the balance of power in favour of the individual by giving them more explicit rights over the processing of their personal data". In practical terms, this means giving data subjects the right to object to certain processing, and the need to view express consent in the context of the bargaining power which the data subject holds.

Advice for Organisations Which Process Big Data

The Report discusses a number of tools that can be utilised in order to ensure that data privacy rights are respected and that data protection principles are complied with when data is processed. One such tool is the use of privacy impact assessments ("PIAs"). These are used to assess whether the processing is fair, and to what extent the individuals whose data is being used are likely to be affected. In February 2014, the ICO published a code of practice giving practical advice on how to conduct PIAs[5] (*see analysis at WDPR, April 2014, page 17*), which is linked to standard risk management methodologies. The Report also discusses the use of privacy by design solutions, which includes measures such as anonymisation techniques, access controls and audit logs, and also data segregation. This approach seeks to find a way to build privacy controls into systems from the outset.

As discussed above, the Report notes the importance of transparency with regards to data collection and data processing, with particular emphasis on the need for privacy notices. The arguments sometimes given against the use of privacy notices with regards to big data analytics (*e.g.,* that the algorithms used in big data are too difficult to explain in simple terms, *etc.*) are also discussed in some depth and countered.

The Report looks at the approach taken by companies in response to big data, and gives examples of companies that have implemented a framework to deal with the issues which arise from it. Aimia, a company that operates in the customer loyalty sector, has developed its own set of data values, symbolised by the acronym "TACT" — Transparency, Added value, Control and Trust. IBM is another company that has developed its own ethical framework, which takes account of issues such as the reliability of data and the consequences of processing. These companies have developed internal policies using their own initiative (and not just as a result of statutory obligations). Despite this, the Report notes that many of their aspects echo the data protection principles which are contained within the DPA.

Conclusion

In summing up the Report, and the current approach of the ICO to big data analytics, it is perhaps appropriate to draw on one of the Report's paragraphs:

> Our view is that the basic data protection principles already established in UK and EU law are still fit for purpose in the big data world. The view that current data protection principles are not adequate underestimates their inherent flexibility. Applying those principles involves assessing the impact of the processing on individuals and whether it is proportionate to the aim being pursued in any particular case. It is true that the current European data protection law was drawn up in the early days of the internet and it is right to look to update it to take account of how personal data is processed now. However, this does not mean that basic data protection principles are no longer fit for purpose in the big data world, or that a new data protection paradigm is required. Big data is not a game that is played by different rules. (paragraph 130)

It is clear that the ICO considers the current legal and regulatory landscape as being fit for purpose in the age of big data. Therefore, it is important that organisations using big data analytics do so by reference to the data protection principles of the DPA, and perhaps consider mechanisms, and implement policies, by which they can ensure effective compliance in this brave new world.

NOTES

[1] EU Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation", available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[2] See http://dynamicinsights.telefonica.com/488/smart-steps.

[3] U.K. Information Commissioner's Office, "Anonymisation: managing data protection risk code of practice", available at http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf.

[4] U.K. Information Commissioner's Office, "Proposed new EU General Data Protection Regulation: Article-by-article analysis paper",

   ISSN 1473-3579

available at http://ico.org.uk/news/~/media/documents/library/Data_Protection/Research_and_reports/ico_proposed_dp_regulation_analysis_paper_20130212_pdf.ashx.

[5] U.K. Information Commissioner's Office, "Conducting privacy impact assessments code of practice", available at http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf.

The ICO report "Big data and data protection" is available at http://ico.org.uk/news/latest_news/2014/~/media/documents/library/Data_Protection/Practical_application/big-data-and-data-protection.pdf.

Emma L. Flett and Ben Robson are Associates at Kirkland & Ellis International LLP, London. They may be contacted at emma.flett@kirkland.com and ben.robson@kirkland.com.