DechertOnPoint

July 2007 / Issue 3

A legal update from Dechert's Data Protection and Privacy Group

European Data Protection Authorities Provide New Guidance on "Personal Data"

Introduction

Data protection law protects the privacy of "personal data", however this term is deceptively simple. A number of factors have recently highlighted the difficulties in defining it, including the advent of new technological advances, the techniques of "de-identifying" data, and an increase in attempts to use data protection law for purposes for which they were not originally designed (at least in the UK). Those holding data, individuals and regulators alike, often struggle in determining when a particular piece of information should be considered personal data. The issue is fundamental. If data is not "personal data", data protection regimes do not generally apply. To name but two consequences: the subjects of that data would not have rights to access it and the controllers of that data would not need to worry about transferring it outside the EEA.

On 20 June 2007, the Article 29 Working Party, made up of data protection authorities from European member states, took the discussion of these issues a major step forward when it issued guidance on the meaning of "personal data". The objective is to provide a common understanding throughout the Member States as to the meaning of this important term, which essentially defines the scope of data protection. Unfortunately, at least in the UK, as we will see, the position is arguably more confusing than ever.

The Working Party points out that the European lawmakers behind the Directive intended to adopt a broad notion of personal data, but that this notion is not unlimited. The Working Party reminds us that the objective of the rules contained in the Directive is to protect the fundamental rights and freedoms of individuals, in particular their right to privacy, with regard to the processing of personal data. These rules were therefore designed to apply to situations where the rights of individuals could be at risk and hence in need of protection. The scope of the data protection rules should not be overstretched, but unduly restricting the concept of personal data should also, they say, be avoided.

As will be seen below, the approach taken by the Working Party to the meaning of "personal data" is markedly different (and wider) from the one adopted by the English Court of Appeal in *Durant v FSA.*[1] The Working Party does not mention *Durant* in its guidance, but it is clear the decision was one of the main reasons they undertook the exercise, and they do expressly disapprove of one part of the *Durant* rationale: the so-called "focus" test.

The Directive

The Data Protection Directive (Directive 95/46/EC) (the "Directive") defines personal data as:

> *Personal data shall mean any information relating to an identified or identifiable natural person ("data subject"); 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 Working Party has focussed its guidance on four elements of this definition: (1) *information*, (2) *relating to,* (3) *an identified or identifiable* (4) *natural person*. It is the second (the subject of the *Durant* case) and third of these requirements which present the greatest difficulties.

[1] Durant v Financial Services Authority [2003] EWCA Civ 1746.

"Information"

The Working Party has given this term a wide interpretation, including both subjective and objective information, e.g., opinions and assessments as well as factual statements.

Information "*relating to*"

According to the Working Party, information can be considered to "relate" to an individual when it is about that individual. Although whether information relates to an individual often involves only a simple assessment, there are other circumstances where the assessment is more difficult. It is this part of the definition of personal data that the *Durant* case was concerned with. The UK Court of Appeal stated that data will relate to an individual if it "is information that affects [a person's] privacy, whether in his personal or family life, business or professional capacity". As the UK ICO subsequently commented in its guidance on the issue,[2] this suggested that, where it was not clear whether information related to an individual, account should be taken as to whether or not the information in question is capable of having an adverse impact on the individual.

The court identified two notions that may assist in determining whether this was so: "The first is whether the information is biographical in a significant sense, that is, going beyond the recording of [the individual's] involvement in a matter or an event which has no personal connotations". The second concerns "focus". "The information should have the [individual] as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest".

The Working Party's guidance states that information which, in the first instance, concerns an object, can relate indirectly to an individual where, for example, the object belongs to someone, or may be subject to particular influence by or upon individuals or may maintain some sort of physical or geographical vicinity with individuals or with other objects. Similarly, where the data are about processes or events, this may still be personal data.

The Working Party has suggested that for data to "relate" to an individual, either a **"content"** element or a **"purpose"** element or a **"result"** element should be present.

According to the Working Party:

- The **"content"** element is present in those cases where information is given about a particular person, regardless of any purpose on the side of the data controller or of a third party, or the impact of that information on the data subject. Information "relates" to a person when it is *about* that person, and this has to be assessed in the light of all circumstances. For example, the results of medical analysis clearly relate to the patient, or the information contained in a company's folder under the name of a certain client clearly relates to him.

- A **"purpose"** element can be considered to exist when the data is used or is likely to be used, taking into account all the circumstances, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual.

- A **"result"** element is present where the use of data is likely to have an impact on a certain person's rights and interests. It was noted that it is not necessary that the potential result be a major impact. It is sufficient if the individual may be treated differently from other persons as a result of the processing of such data.

As a result of the "content", "purpose", or "result" analysis, the same piece of data could feasibly relate to different individuals. The same information may relate to individual A because of the "content" element (the data is clearly about A), and to B because of the "purpose" element (it will be used in order to treat B in a certain way), and to C because of the "result" element (it is likely to have an impact on the rights and interests of C).

Importantly, and in contrast to the view taken in the UK after *Durant*, it is not necessary for the data to *focus* on someone in order for it to be considered to relate to him.

The Working Party has pointed out that the fact that the same piece of information may relate to more than one individual should be borne in mind when data protection principles are being applied, particularly the right of subject access.

[2] Guidance: The *Durant* Case and its impact on the interpretation of the Data Protection Act 1998, 27/02/06.

An *"identified or identifiable"* Natural Person

The Working Party has stated that in general terms, a natural person can be considered as "identified" when, within a group of people, he or she is "distinguished" from all other members of the group. A person is "identifiable" if it is possible to identify him, albeit that the process of so identifying him has not yet taken place.

Examples of identifiers which allow the process of identification to take place are mentioned in the definition of "personal data" in Article 2 of the Directive where it states that a natural person *"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"*.

Whether a particular identifier will be capable of identifying a person will depend on the particular situation. A very common family name will not be sufficient to identify someone—i.e., to single someone out—from the whole of a country's population, while it is likely to achieve identification of a pupil in a classroom. Even ancillary information, such as "the man wearing a black suit" may identify someone out of the passers-by standing at a traffic light.

According to the Directive, when determining whether a person is identifiable, account should be taken of all the means likely reasonably to be used to identify the person. This means that a mere hypothetical possibility to single out the individual is not enough to consider the person as "identifiable". When thinking about what means are likely reasonably to be used, the cost of conducting identification is one but not the only factor. Others include the intended purpose, the way the processing is structured, the advantage expected by the controller, and the interests at stake for the individuals, as well as the risk of organisational dysfunctions and technical failures.

In some circumstances, the sole purpose of processing information is to allow the identification of specific individuals and treatment of them in a certain way. 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. Therefore, in these circumstances, the information should be considered as relating to identifiable individuals and the processing should be subject to data protection rules.

If the identities of the individuals to which information relates are disguised, is the information personal data? This will depend on at which stage the disguising is used, how secure it is against reverse tracing, the size of the population in which the individual is concealed, the ability to link individual transactions or records to the same person, etc. If information is truly anonymous and the identification of the individuals to which it related is no longer possible, it will not be personal data.

"Natural Person"

The Directive only applies to natural persons, e.g., human beings. As well as pointing out that national law may extend the application to unborn children as well as deceased persons, the Working Party points out that although the Directive only applies to natural persons, nothing prevents the Member States from extending the scope of their data protection laws to areas not included within the scope of the Directive. Accordingly, some Member States such as Italy, Austria, and Luxembourg have extended the application of certain provisions of national law adopted pursuant to the Directive (such as those on security measures) to the processing of data on legal persons (i.e., corporate entities). As in the case of information on dead people, when a controller simply does not know that a person is dead, practical arrangements by the data controller may also result in data on legal person being subject *de facto* to data protection rules.

Conclusion

The Working Party clearly hopes that its note provides helpful guidance on the current thinking in relation to personal data in the various Member States. However, for controllers in the UK at least, the position is arguably more confusing than previously. A few points:

First, whilst the guidance is clearly intended to be a statement of wide definition, and there is an express rejection of a "focus" test, it is interesting to speculate how Mr. Durant would have fared had the English courts applied a test along those lines (It is unfortunate, albeit given considerations of comity perhaps understandable, that of the many examples given in the opinion, none involved facts which shed any light on a *Durant*-type situation). It will be recalled that Mr. Durant made a data protection subject access request to the Financial Services Authority seeking information concerning litigation

between himself and Barclays Bank. This request was refused on the grounds that the information was not personal data as the information did not have Mr. Durant as its focus. The information sought included correspondence between the FSA and Barclays Bank, in which correspondence Mr. Durant's name appeared; nonetheless, the court felt that it was information about (or focussing on) either his complaints or Barclays Bank and the FSA who were involved in resolving his complaints (not about, or focussing on, him).

The Working Party equates "relates to" with "about", which is fine, but they do then of course recognise that that latter term itself needs expansion; hence the introduction of the three alternative elements "content", "purpose" and "result". Applying these to Mr. Durant:

- The "content" test is fulfilled when the information is "about" the individual and (leaving aside the circularity) does not really help Mr. Durant; the courts found the information to be about his complaint (or Barclays or the FSA), not about him.

- The "purpose" test is fulfilled when the data is to be used with the purpose of evaluating, treating in a certain way or influencing the status or behaviour of an individual. Mr. Durant might fare better under this test. Would correspondence between FSA and Barclays (or internal FSA minutes) be used by the FSA to determine how they would treat Mr. Durant? Arguably so. But equally arguably not, as FSA's purpose is not to evaluate, treat in a certain way or influence the status of behaviour of Mr. Durant at all; the FSA was processing the information for the purpose of investigate *his complaints* and, arguably, he is mentioned in the internal documents and correspondence at issue only as instigator of the complaint.

- Lastly, the "result" test will be fulfilled if use of the data is likely to have an impact on Mr. Durant's rights and interests. Again, arguably this would be fulfilled as the outcome of the complaint would possibly have had such an impact. The contrary view is that it is surely not all rights and interests that should be taken into consideration, but only those which impact the purpose of the Directive; namely, the individual's right to privacy (a consideration which the UK court in *Durant* had firmly in mind).

Secondly, although the regulators here are espousing the widest of possible interpretations of the definition of personal data, it is not necessarily the case that when the issue reaches the ECJ (as it must surely do some day) that the court will agree with them. Prior to the *Lindqvist* case,[3] for example, many considered that putting information on a web site so as to be accessible from outside the EEA would automatically be a transfer out of the EEA. The ECJ in *Lindqvist* shows that that was too simplistic a view.[4]

Lastly, the Working Party's opinion, although important, is not binding. It must be borne in mind that the constituent members are the data protection authorities, the persons charged with enforcing data protection law; they do not make the law. This point is likely to loom large in the UK. The internal deliberations of the Working Party are unfortunately not published, and Article 29 of the Directive makes it clear that majority decisions are all that are required; given the difficulty the UK now finds itself in, one wonders how the UK ICO voted. In the meantime, the UK courts and the UK ICO at least are bound by the *Durant* decision and the "focus" test set out in that decision. It will be interesting to see the UK ICO's reaction to this opinion. It is understood that new revised guidance will be published by the ICO; the ICO having stated that he considers it is possible to reconcile to this opinion with *Durant*.

■ ■ ■

This update was authored by Renzo Marchini and Kate Tebbutt.

[3] *Bodil Lindqvist v Kammaraklagaren* (ECJ 2003, Case C-101/-1).

[4] A transfer only occurs, said the ECJ, when someone outside the EEA actually accesses the information.

Practice group contacts

If you have questions regarding the information in this legal update, please contact the Dechert lawyer with whom you regularly work, or any of the lawyers listed.
Visit us at www.dechert.com.

Olaf Fasshauer
Munich
+49 89 21 21 63 21
olaf.fasshauer@dechert.com

Pierre Louis
Brussels
+32 2 535 5479
pierre.louis@dechert.com

Renzo Marchini
London
+44 20 7184 7563
renzo.marchini@dechert.com

Giovanni Russo
Munich
+44 20.7184.7310
giovanni.russo@dechert.com

Jonathan Schur
Paris
+33 1 53 65 05 10
jonathan.schur@dechert.com

Jean-Yves Steyt
Brussels
+32 2 535 5425
jean-yves.steyt@dechert.com

Kate Tebbutt
London
+44 20 7184 7518
kate.tebbutt@dechert.com

Benedikte Verdegem
Brussels
+32 2 535 5440
benedikte.verdegem@dechert.com

Dechert LLP
www.dechert.com

UK/Europe

Brussels
London
Luxembourg
Munich
Paris

U.S.

Austin
Boston
Charlotte
Hartford
New York
Newport Beach
Philadelphia
Princeton
San Francisco
Silicon Valley
Washington, D.C.