Re-defining "personal data" — can the opinion live up to the hype?

Dan Cooper, of Covington & Burling LLP, comments on the Article 29 Working Party's re-definition of "personal data" and discusses the impact it will have on organisations

The long-awaited opinion paper, exploring the concept of "personal data," was finally released by the Article 29 Working Party on 27th June 2007('WP 136') and its ramifications are still being felt. The concept of "personal data" is fundamental to the EU framework Data Protection Directive 95/46/EC ('the Directive') and individual Member State data protection statutes, including Ireland's Data Protection Acts 1988 and 2003.

The paper had been eagerly anticipated by industry, which hoped that a number of simmering debates over the appropriate scope and application of EU data protection laws might have been resolved.

In WP 136, the Working Party explore the concept of "personal data" by analysing four different elements of the definition appearing in the Directive. Article 2(a) of the Directive provides that:

"*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*."

Background

The Working Party's principal motivation in issuing WP 136 was to harmonise divergent interpretations of the concept of "personal data" across the EU, and provide some practical guidance on how the concept of "personal data" should be understood in concrete cases. At present, there are significant differences in the way EU data protection authorities have defined the term "personal data." This inevitably has led to divergent applications of national data privacy statutes within the various Member States. For example, some Member States disagree over whether an objective or subjective standard should be applied when determining whether or not information is personal.

- **Subjective approach:** information is only considered "personal data" where the organisation in possession of that information is able to directly or indirectly identify a natural person. This identification can arise from the information alone, or from the information combined with other details that the organisation may possess or may reasonably be able to acquire.

- **Objective approach:** this approach gives rise to a more expansive application of data privacy laws. It allows information to be considered "personal data" where any organisation, whether it be the organisation actually possessing the information or any other party, can attribute the information to a living individual.

Needless to say, such fundamental differences over how the concept of "personal data" should be understood have proven particularly problematic for large international organisations who operate across a range of Member States and are exposed to multiple data protection laws.

Analysis of the Working Party opinion

The Working Party's opinion is divided into four sections, which reflect the different elements of the definition of "personal data" in the Directive; namely:

(i) any information;
(ii) relating to;
(iii) an identified or identifiable;
(iv) natural person.

Critically, the belief that European law makers intended there to be a "wide notion of personal data" shapes much of the Working Party's analysis.

It is understandable that the Working Party would instinctively prefer that the notion of "personal data" be understood in a "wide"

(Continued on page 8)

(Continued from page 7)
sense, if only to avoid limiting national data protection laws through a narrow understanding of the term. Yet, the clear disadvantage to a wide definition is that it allows national data protection authorities to develop and apply potentially inconsistent interpretations of the term in their respective jurisdictions. Thus, the Working Party's aim to harmonise understanding and application of the term in the EU is effectively doomed from the outset.

" Videotapes of CCTV camera images, audio recordings from call centres, and electronic mail will all contain information that qualifies as personal data."

"Any information"

The Working Party states that when assessing the phrase "any information," both the content of information, and its format, need to be referenced.

In terms of content, the opinion notes that both objective information (for example, facts about a person's physical make-up) and subjective information (for example, an expression of an opinion about the person) fall within the definition of "personal data." Furthermore, information does not have to be factually correct — an expression of a judgment, whether truthful or not, about an individual, is also "information."

Regarding format, information can take a variety of forms, including numerical, alphabetical, graphical, or acoustic. Videotapes of CCTV camera images, audio recordings from call centres, and electronic mail, will all contain information that qualifies as "personal data." The Working Party's analysis of CCTV images could prove worrying to some, since it suggests that organisations must fulfil the full range of data privacy duties with respect to individuals with whom they have only a fleeting or (for external CCTV cameras) no business relationship.

The opinion does attempt to qualify this interpretation slightly by noting that *"images of individuals captured by video surveillance can be personal data to the extent that the individuals are recognisable."* However, the Working Party critically fails to mention to whom the person must be recognisable — the CCTV operator, the individual's friends and family, or another person.

Biometric data and DNA are also considered "personal data," although tissue samples from which DNA can be derived are not "personal data" themselves — they are merely the "sources" from which "personal data" can be obtained.

This concession will be of interest to those organisations and research institutes operating 'bio banks' and collecting tissue samples for research purposes.

"Relating to"

Besides observing that information will be considered to "relate to" an individual when it is about that individual, the Working Party notes that often data may not relate directly to an individual, but could relate to an object (for example, the price of a house or the IP address of a computer) that bears some relation to the individual.

Controversially, the Working Party takes the view that information can "relate" to an individual where there is either a content element, a purpose element, or a result element. Taking each in turn:

- **Content:** the "content" element will be present in cases where the information is clearly about the individual. This has to be assessed in light of all the circumstances surrounding the case, for example, information contained in medical records and employee files will clearly be about an individual.
- **Purpose:** the "purpose" element will be present when the information is used or is likely to be used for the purpose of evaluating, treating in a certain way, or influencing the status or behaviour of an individual.
- **Result:** a "result" element will be present where the use of the information will have an impact on a person's rights and interests, taking into account all the circumstances surrounding the case. The Working Party notes that it is not necessary for the information to have a significant impact upon the individual: *"it is sufficient if the individual may be treated differently from other persons as a result of the processing of such data,"* which may cause concern for organisations processing data.

Given that any of the above three factors can lead to information being held to "relate to" an individual, information that might not intuitively be regarded as "personal data" is likely to fall within the scope of EU data protection laws. Although it is understandable that the Working Party has sought to adopt an expansive interpretation of the phrase, industry could be forgiven for thinking that it has gone too far.

While the "content" element should present fewer difficulties because it is tied more closely to conventional beliefs about what are "personal data," the "purpose" and "result" elements will prove more problematic.

According to the Working Party, the purpose element is satisfied whenever information is used to *"evaluate, treat in a certain way or influence the status or behaviour of an individual."* This could conceivably cover a wide range of information. For instance, the Greater London Authority has imposed a traffic congestion charge that dissuades many individuals from driving to work. This decision has "influenced" behaviour, but then does information possessed by the authority and relating to this scheme qualify as "personal data" relating to individuals? Although the result seems absurd, the Working Party's loose language arguably points in that direction.

The "result" element is potentially even more problematic, since a variety of factors, and organisations, influence our lives every day to differing degrees. National and local governments make decisions, legislatures enact laws, companies market goods and products, and employers issue policies that affect employees every day — sometimes in a very direct and targeted fashion. Although the Working Party cautions that the information should result in the individual somehow being treated differently from others, it fails to clarify where the line reasonably should be drawn.

"An identified or identifiable"

The "identified or identifiable" aspect of the definition remains perhaps the most controversial component of the paper. The Working Party, notes among other things, that:

(a) even if a person is not named, he/she can be identifiable on the basis of socio-economic or other criteria, such as age, occupation, place of residence, that relate to a person and can, collectively, become identifiable;

(b) the possibility of identifying an individual must be seen in light of *"all the means likely reasonably to be used either by the controller or by any other person to identify the said person"* (quoting Directive, Recital 26); and

(c) in assessing "all the means likely reasonably to be used," the purpose of the processing will play an important role; data processing operations that envision — or potentially are based on a desire to achieve — the identification of a person, will most likely convert information into "personal data."

It is reasonable for the Working Party to conclude that information does not have to refer to a person by name for it to be "personal data." The Working Party state that the test to be applied is a "dynamic one." In effect, organisations collecting information that is not "personal data," but potentially could be, must constantly assess whether changes in technologies, disclosures of information by third parties, or other factors thereby have converted the information into "personal data."

Organisations could find information that they have held for years is suddenly transformed into protected "personal data," with all of the associated legal ramifications.

"It is reasonable for the Working Party to conclude that information does not have to refer to a person by name for it to be 'personal data'."

Further, the opinion states that when assessing "all the means likely reasonably to be used," one of the key factors will be the purpose pursued by the organisation in processing the information. The Working Party notes that if an organisation maintains the intent, at some future time, to attribute information to an individual, then the information is likely to be "personal data." The potential ramifications of this analysis are troubling, since it ignores whether, in fact, the company — in objective terms — actually can or will be able to establish such a link.

The Working Party explains, by way of example, that if a transportation firm, in order to combat graffiti, prepares a register containing images of each graffiti artist's "tag" or signature," then this information would constitute protected "personal data." This is so because the firm's purpose is to "identify individuals to whom the information relates" in order to assert legal claims — it is irrelevant whether identification is likely to occur.

An organisation could rightly question how it is meant to comply with the various duties and responsibilities applicable to a data controller in these circumstances. For example, is it reasonable to expect notices to be displayed to persons generating the graffiti, or will some regulators conclude that the information is sensitive "judicial data" because it relates to the commission of an offence?

Many organisations hold information that, in an ideal world, they would like to know to whom it relates. But, mere subjective intent seems hardly sufficient to conclude that the information qualifies as "personal data."

The Working Party also appears willing to apply the phrase "identified or identifiable" expansively when analysing the notion of "personal data." For instance, various examples given in the paper reveal that where an organisation holds a pool of data, and is deemed capable of attributing a single strand of that data to one individual, then the entire data set is converted to "personal data."

The Working Party explains this principle by using the example of CCTV images — because the very purpose of CCTV is to identify persons captured by the images, it must involve the processing of "personal data, even if some persons recorded are not identifiable in practice."

"Natural person"

The term "natural person" remains the most straightforward part of the definition of "personal data" in the Working Party's analysis.

The Working Party observes that data protection laws apply only to living individuals, thus excluding information relating to deceased persons and, potentially, unborn children. However, the Working Party allows that different countries will establish their own rules for deciding at what point in time an unborn child qualifies for legal protection as a living human being, with some countries willing to extend protections at an earlier stage than others.

In addition, the Working Party notes that in some cases, information about a deceased person can still enjoy the same protections that are extended to data relating to a living person. In some instances, a controller may not be able to tell whether a person is alive or dead and so, as

(Continued on page 10)

(Continued from page 9)
a precaution, will need to process the information as though it were "personal data."

Information about a deceased person also may qualify as "personal data" if it relates to another living person. For example, where an individual dies of a hereditary disease, information about the condition would qualify as "personal data" with respect to the person's blood relations.

Implications for industry

Given the nature of the topic, the Working Party's opinion is likely to be relevant to nearly every organisation that processes "personal data." However, certain key industries are likely to find the paper to be particularly relevant, notably those that routinely deal in information that exists at the periphery of what is understood today to be "personal data."

Judging by the examples and substantive discussions used, the Working Party appear to have had certain industries and activities in mind when preparing the paper.

Pharmaceutical research

The Working Party take pains to address existing uncertainties surrounding the status of the key-coded, de-identified trial data, which is collected and processed in the clinical trial context. Unfortunately, various ambiguities in the Working Party's discussion leave the status of such data ultimately uncertain.

On the one hand, the Working Party steers towards a conclusion that key-coded data are "personal data," on the contentious basis that one of the chief purposes of key-coding such data is to assist in the re-identification of the individual in certain contexts. But, one could equally argue that the purpose of key-coding — at least from the trial sponsor's perspective — is to achieve precisely the opposite result, namely to avoid learning the actual identity of the underlying patient.

On the other hand, the Working Party make statements that go in the opposite direction. For instance, we learn that where study protocols and procedures exclude re-identification of the trial subject, then it may be possible to conclude that key-coded trial data are not "personal data." More surprisingly (and in a far cry from its earlier analysis of IP addresses and CCTV images), the Working Party are prepared to stick with this conclusion even where identifying some of the trial subjects takes place in spite of such protocols and procedures.

Elsewhere, the analysis becomes even more uncertain, as the Working Party suggests that key-coded data might somehow occupy a middle ground between personal and non-personal data after concluding that the data may be eligible for "more flexible" treatment under national data privacy rules.

Rights holders

Another group likely to find the Working Party paper of interest is IP rights holders, particularly those engaged in online right enforcement efforts that often involve the collection and analysis of Internet user data, such as IP addresses, in order to detect infringing conduct. Regulators have examined such activities in the past and they continue to remain controversial when conducted in Europe. In its opinion paper, the Working Party once again reiterates its view that in most instances IP addresses are data relating to identifiable individuals and hence are classed as "personal data." In reaching this result, the Working Party emphasise the purposes for which rights holders gather IP addresses — which it takes to be the identification and prosecution of infringers — rather than whether the identification of the ultimate user is a realistic possibility.

However, rights holders could rightly ask whether this analysis would apply where their principle purpose in processing IP addresses is more conservatively to direct ISPs to issue notice-and-takedown requests on the rights holders' behalf and not to learn the user's identity.

Radio frequency identification technologies

With respect to radio frequency identification ('RFID') technologies, the Working Party opines that data contained in an RFID chip or tag on an identity document (like a passport) will be considered to 'relate' to that person, and so are likely to fall within data protection laws. Perhaps more significantly, the Working Party notes in its conclusion, that it intends to produce additional guidance as to whether, and to what extent, EU data protection rules interact with RFID technologies. Organisations that currently make use of such devices will want to remain vigilant for further developments. This journal will publish an update on this issue as soon as it is available.

Conclusion

The Working Party's opinion on the concept of "personal data" is a commendable attempt to provide further insight and clarity into the often nebulous issue of "personal data," and by extension, how EU data protection law should be applied in practice.

The opinion provides useful information regarding the basic components of the definition, and how each part should be analysed. However, the opinion stops short of providing firm guidance that would be both useful to industry and create uniformity of opinion amongst EU data protection regulators. Ultimately, the Working Party appears to have deferred the hard task of compelling individual EU data protection authorities to adopt a truly uniform position on the subject, which means a tough road ahead for industry. Indeed, it could be suggested that the best strategy for organisations doing business in the EU after the Working Party paper is, quite simply, wait and see.

Dan Cooper
Covington & Burling LLP
dcooper@cov.com