

some regulators. The CNIL is now inspecting the data protection practices of businesses without prior notice. The UK Commissioner has begun obtaining formal written undertakings from businesses found to be in breach of data protection laws, and requiring them to remedy deficiencies and to submit to audits of their data protection practices. In the overall scheme, however, these enforcement tools reflect the creative initiatives of individual regulators rather than a concerted attempt to enforce key data protection regulations.

**Risks of change**

There may be dissatisfaction with the status quo, but there are also risks associated with change. If we move away from a consent-centric system of governance to one based on another variable, will consumers lose the limited control they have today? Will the private, indi-

vidual space which Alan Westin described as a necessary and universal cultural value shrink even further?

Businesses have found a way of operating within the current regulatory structure. The approaches they have adopted may not be perfect, but the majority seek to behave responsibly and to respect privacy norms. Many would probably favour maintaining the status quo on the basis that changing compliance systems is expensive and uncertain.

**The challenge**

The challenge for each of us is to encourage an honest and open dialogue about these issues. Privacy is a cultural value, and privacy-related laws need to reflect our wider societal concerns and aspirations. New influences, such as technological advances, data mining and data analytics, anti-terrorist surveillance, and medical research must be weighed against

the risks to society if the curious succeed in further reducing the individual private sphere which each of us needs.

These issues are being debated now and will be debated in the coming years. Privacy laws are being revisited around the world. The Australian Law Reform Commission report, due in final form in February, is one of many examples. There are also private sector privacy efforts under way to green field information policy. We all need to contribute to this debate.

© *Hunton & Williams*

**AUTHORS**

Martin Abrams is Executive Director, Centre for Information Policy Leadership, Hunton & Williams, e-mail: mabrams@hunton.com

Bridget Treacy is a Partner at Hunton & Williams, London, e-mail: btreacy@hunton.com

# New interpretation of ‘personal data’ may affect subject access

According to the ICO, any information that ‘relates to’ an individual may need to be provided in a subject access request. Practical difficulties lie ahead for businesses in deciding to what extent video images of general crowd scenes, for example, should be provided. By **Gary Brooks**.

As reported in the September issue of the *PL&B UK* newsletter (pp.10-11), the Information Commissioner’s Office (ICO) has issued new guidance on what constitutes “personal data”. This guidance from the regulator seeks to update the previous version, which centred on the narrow interpretation of the concept decided by the Court of Appeal in *Durant v Financial Services Authority*. This article examines the practical implications of the new regulatory approach in the UK and whether the ICO has succeeded in making the position clearer.

**Introduction**

So, what is personal data exactly? The precise interpretation of this concept is vital as it ultimately determines the extent of the practical data protection obligations faced by all UK businesses. Yet, remarkably, it still remains very difficult in some circumstances to decide

when a piece of information is caught by the legislation and when it falls outside.

The ICO guidance follows the recent Opinion adopted by the influential EU Article 29 Data Protection Working Party which was produced in an effort to come to a common understanding of the concept of personal data across the EU Member States. The Article 29 Opinion adopts a broader interpretation of the concept than the UK’s *Durant* approach and “reflects the intention of the European lawmaker for a wide notion of personal data”.

The ICO guidance is an attempt in the Commissioner’s own words to “square the circle” and reconcile the two positions, although it generally follows closely the broader approach taken by the Article 29 WP paper. This is not surprising, particularly as this issue of the UK’s narrow interpretation of the concept as set out in *Durant* is believed to be one of the areas which

the European Commission is examining as part of its ongoing investigation into whether the UK has implemented the Data Protection Directive correctly.

To understand the changing regulatory landscape, it is necessary to revisit briefly *Durant* as the leading UK data protection case. The Court of Appeal said that in order for information to constitute “personal data”, the information must affect a person’s privacy (in either his personal or professional life). In deciding whether an individual’s privacy was affected, the Court said that two notions may be of assistance. Firstly, whether the information is biographical (i.e. it must go beyond a passing reference to the individual’s name in a matter that has no personal connotations) and, secondly, whether the individual is the focus of the information, as opposed to the focus being some other event with which he may be connected.

How is compliance with data protection obligations affected? Here are four initial observations:

**1. *Durant* remains good law!** An obvious yet important point is that the Court of Appeal's interpretation in *Durant* (as applied in subsequent cases) remains good law in the UK and that the guidance is not legally binding. There is some justification therefore in carrying on as normal for all activities until such an approach is challenged. However, in practical terms, it is the ICO as the data protection regulator that businesses have to deal with in the event of a data protection complaint or investigation. The regulator's interpretation of personal data (and how *Durant* fits into the concept) cannot realistically be ignored when things go

wrong. Companies are generally best advised to adopt the safest highest common denominator approach to this issue by considering any information which relates to an individual (whether directly or indirectly) to be subject to the company's security and retention standards, not least because it is impractical to engage in a painstaking analysis of whether each particular document/set of data has a sufficient degree of proximity to the individual so as to qualify as personal data.

**3. When dealing with contentious subject access requests, more borderline information is likely to be covered.** Some businesses are already struggling to apply the new guidance in the context of responding to subject access requests for borderline informa-

tion instead be seen to take a robust approach to security and records management. In matters of data security and data disposal, it is usually safer to treat all types of information as if it were personal data.

### How to make a decision in borderline cases

The definition of personal data has four elements set out in the Article 29 Opinion, which are effectively incorporated into the ICO guidance:

- "any information"
- "relating to"
- "an identified or identifiable"
- "natural person"

### Any information

We are going to focus on the "relating to" element as that is where the most significant changes lie, and it forms the crux of the guidance. But it is worth mentioning one point in connection with the first element. This is that the Article 29 Opinion confirms that false information can count as personal data. This is particularly important in the developing online world and for social networking websites in particular, where users of such sites can easily post false information about other individuals on their profile pages which could potentially cause damage or distress to such individuals. The victims therefore potentially have data protection rights in this false information.

### Relating to

The guidance provides a number of useful practical examples and a form of questionnaire/flowchart to help the reader decide if a particular piece of information "relates to" an individual. These will be considered briefly below in conjunction with the equivalent guidance from the Article 29 WP opinion. With each question below, if the answer is "Yes," then the information is personal data, and if the answer is "No," you go to the next question. If the answer to the last question is "No," the information according to the guidance is "unlikely to be personal data".

- Is the information "obviously about" the individual or clearly linked to him? As an example, the information recently lost by HM Revenue and Customs is personal data because it is either obviously

---

## The ICO's new interpretation will not have a huge impact on the data processing operations of most businesses.

---

wrong and a letter from the ICO lands on your desk.

**2. Carry on as normal for most data processing activities.** Generally, it is obvious whether a particular piece of information qualifies as personal data, because the content of the information will be about the individual or their activities (e.g. a name, address, e-mail address, medical record or information about an individual's performance at work). To that end, the Information Commissioner's new interpretation will not have a huge impact on the data processing operations of most businesses since most data processing activities will obviously fall within the scope of the definition. For example, carrying out a direct marketing campaign to individuals on your customer database will involve using their addresses, phone numbers and e-mail addresses, which qualify as personal data because they can be linked to an identifiable individual.

Similarly, it is not likely to change how businesses comply with other key data protection obligations, including, for example, how they decide which types of information should be covered by their data retention and data security

tion (such as e-mails), not least because if you follow the Information Commissioner's new flowchart for borderline cases where the information concerned is not obviously personal data, it is very hard to reach a conclusion that the information concerned is not personal data. This is discussed in detail below.

**4. Data that falls outside the definition still worthy of some protection.** Prudent businesses are already aware that information which does not quite fall within the concept of "personal data" is usually still worthy of some level of protection. For example, it would be risky for a company in the event of a data security breach (involving information which only indirectly relates to individuals) to seek to rely on a technical argument that it did not have to afford any protection to the data in that situation because it does not strictly qualify as personal data. Even if not strictly personal data, other sets of rules may come into play here, such as the Article 8 right to respect for private and family life, criminal law or the rules of other regulators such as the Financial Service Authority, or even pure commercial considerations of wishing to avoid bad publicity and

about or linked to the individual (e.g. name, address and information such as National Insurance number and bank account details that can be linked to an identifiable individual).

- What is the purpose of the data processing? Is the data used or is it to be used to inform or influence actions or decisions affecting and identifiable individual?

The key question here is whether the data is used (or likely to be used) to learn something about the individual or to determine something about him? This is a new and potentially very broad condition and it involves a degree of subjectivity.

An example is given in the guidance of two photographers taking almost identical photographs of revellers at a New Year celebration in Trafalgar Square. One photographer is a journalist taking the photo for his own archive library, the other is a police officer taking photos of the general crowd scene to identify potential troublemakers. In the hands of the journalist, the photo is not personal data as it is not being used to learn anything about an identifiable individual. However, the photo taken by the police officer may contain personal data as it was taken for the purpose of recording the actions of individuals whom the police would seek to identify in the event of trouble so that they can take action against them.

- Does the information have any biographical significance in relation to the individual? This is the first of the *Durant* principles, as described above. The Commissioner seems to be taking a broad approach to this in the guidance by interpreting biographical significance as simply whether the data has any personal connotations. An example given in the guidance is of meeting minutes showing that an individual attended. The fact that the individual attended at a particular time and place is biographical and qualifies as personal data. The rest of the minutes are unlikely to be personal data about the attendees though, unless they focus on such individuals (see next question).
- Is the individual the focus of the information? This is the second of the *Durant* principles. However,

there is a very significant change as a result of the Article 29 Opinion, which is that information can “relate to” an individual (and therefore qualify as personal data) even if it does not focus on a specific person. If information has qualified as personal data under any of the previous headings, then it is not necessary to consider focus. The previous ICO guidance had stated that “information that has as its focus something other than the individual will not be personal data”. The new guidance correctly recognises that this is not the case, with “focus” simply being one factor which is sufficient for the information to be personal data but one which is not actually necessary in each case. The significance of this change is discussed further in the subject access section below.

- Does the information impact on an individual, whether in a personal, family, business or professional capacity?

There is a degree of overlap here with the “Purpose” test above, and it mirrors the “result element” of the Article 29 paper. The Commissioner says that if there is a “reasonable chance” that the information will be processed to learn, record or determine something about that individual, then it will qualify as personal data, even if it was not the data controller’s intention to process the data for this purpose.

However, this test seems to be very broadly interpreted by the Commissioner from the author’s recent experience, with the Commissioner following the approach of the Article 29 paper, which states that “the impact

information will fall outside the scope of the definition, a point which will be illustrated below.

### Practical implications when responding to subject access requests

The new approach of the regulator on the “relates to” aspect is already having a significant (and potentially adverse) impact on those companies that are faced with difficult and wide-ranging subject access requests. With a recent ICO survey confirming that people are becoming increasingly aware of their data protection rights, certain high profile UK businesses are continuing to deal with growing amounts of difficult requests for “everything about me”, typically on the back of a complaint or grievance by the individual concerned. These requests can on occasion, when dealing with a persistent or vexatious requester, be very difficult and, if the data is not easily accessible, financially very costly to deal with.

Until now, businesses have often been able to take a robust approach based on *Durant* and fend off (at least in part) those wide-ranging requests by stating that the information does not relate to the individual because its focus is not on the individual but on his complaint or the broader matter in which he is involved, and therefore it falls outside his right of access.

The new guidance, however, makes it clear that information can “relate to” an individual (and therefore qualify as personal data) even if it does not focus on a specific person, which can make it hard to decide if certain information is covered. There are likely to be practical difficulties for businesses in deciding to

---

## UK businesses continue to deal with growing amounts of difficult requests for “everything about me”.

---

does not have to be significant, merely that the individual may be treated differently from other people on the basis of that information”.

Having reached the end of the questionnaire, it is hard to see many circumstances where borderline

what extent video images of general crowd scenes (of the type recorded by CCTV) should be provided in response to subject access requests.

Let’s take a hypothetical example. Mr Smith, makes a written complaint to a retailer, having purchased eggs as a

customer which were salmonella-infested. The retailer carries out an investigation into the complaint. Whilst the investigation is ongoing, Mr Smith makes a subject access request to the retailer for “everything you hold about me, including all e-mails and internal correspondence”.

There are internal e-mails between staff members about how to deal with Mr Smith’s complaint, which mention his name. Do these e-mails relate to Mr Smith so as to constitute his personal data? Working through the ICO questionnaire, it is not likely that the content of the e-mails is biographical or focuses on Mr Smith. Rather the e-mails are likely to focus instead on the subject of his complaint.

However, looking at the final question, the data is likely to have an “impact” on Mr Smith’s rights and interests since the outcome of the investigation would have such an impact, even if its purpose was only to evaluate the complaint. It may be then that such information would qualify as personal data (when under *Durant* principles it would clearly fall outside), but the position is not clear and depends on how widely this condition is interpreted.

**Is the new guidance consistent with *Durant*?**

Only in the sense that the *Durant* principles (of biographical significance and

focus) still remain part of the assessment. However, the new ICO guidance envisages information qualifying as personal data even when it does not affect the individual’s privacy, which makes it inconsistent with *Durant* in one major respect. The absence in the guidance of a reference to the core principle in *Durant* that the information concerned must “affect the individual’s privacy” to qualify as personal data is puzzling and suggests that the Information Commissioner does not support this aspect of the *Durant* judgment and is unable to reconcile the Court’s approach on this point with the stance taken by the Article 29 Working Party.

**Conclusion**

The ICO’s new stance is undoubtedly closer to the more logical interpretation of the concept in the Directive. From that perspective, it is to be welcomed. Pan-European businesses will welcome the fact that EU regulators are trying to achieve a common understanding on this issue.

However, it is difficult in certain circumstances to reconcile the new approach as set out in the ICO Guidance with the *Durant* principles (which remain law), and there will still be confusion when dealing with borderline information, particularly when assessing whether information has to be disclosed

in response to subject access requests.

As a consequence of the new broader approach, an individual now has got more scope to make wide-ranging requests in pursuance of a claim or grievance, thereby circumventing the discovery rules and potentially causing significant disruption and expense to the data controller (this is precisely the scenario that led the Court of Appeal to rule against Mr Durant and in favour of the FSA). This is already a real problem for certain high-profile UK businesses.

With an eye on the future, the interpretation of the “relates to” condition will play a vital role in the application of the existing law to new technology, such as RFID. The Information Commissioner and the European Data Protection Supervisor have, however, recently called for a revision of the Directive in five years’ time so that this vital privacy law can seek to catch up with the faster pace of new technology. It therefore remains to be seen how long the current approach will remain in force.

**AUTHOR**

Gary Brooks is a consultant to *Privacy Laws & Business* and others including law firm Berwin Leighton Paisner. e-mail: gary@dataprotected.co.uk

# Appropriate training method guarantees best results

Data protection training is essential for organisations of any size. With courses now readily available online as well as onsite, what factors should privacy officers consider in choosing a delivery method? **Dugie Standeford** reports.

“Data protection is never going to be viewed as the sexiest subject in the world, and attempts to deliver the necessary messages in a formal, rigid, grey manner are unlikely to reach anybody but the pathologically attentive,” says Owen Thomas, Data Protection Officer in the Sunderland City Council city solicitors department.

Like many other employers, the council uses online and onsite training, Thomas says. New staffers are given data

protection basics via an online package, while more bespoke or service-specialised training sessions and materials are delivered through methods ranging from informal “guided discussions” within routine team meetings to face-to-face training aimed at chosen audiences for whom particular risks, interests or concerns have been identified.

The most effective way to “keep snoring at bay” is to tailor the materials to the relevant audience and “try to inject some variety” into the teaching

methods used, Thomas says. Online sessions may reach the “PlayStation generation more effectively than the Baby Boomers”, while face-to-face presentations may be more palatable to older workers. Different approaches make it more likely that the majority of employees will be reachable by one style or another, he adds.

**Online training**

The key to selecting a DP course is to decide “what you want to achieve from

# Your Newsletter Subscription Includes

# e-Newsletter

## 1. Five newsletters a year

The *Privacy Laws & Business (PL&B)* United Kingdom Newsletter's scope ranges beyond the Data Protection Act to include the new Freedom of Information Act, related aspects of the Human Rights Act and the Regulation of Investigatory Powers Act. It also covers Jersey, Guernsey and the Isle of Man. The newsletter complements the International Newsletter which has been the leading data protection and privacy publication for 20 years.

## 2. E-mail updates

We will keep you frequently informed of the latest privacy developments.

## 3. Country, Subject, Company Index

Subscribers will receive annually a cumulative subject index of all topics covered. Multiple headings include advertising, data security, Internet, police, transborder data flows and sensitive data. The index is updated after every issue on our website [www.privacylaws.com](http://www.privacylaws.com).

## Electronic Option

The newsletter is available, for an additional enterprise licence fee, in PDF format for uploading onto your intranet or network. This format enables you to see the newsletter on any screen on your network as it appears in the paper version. It allows you to print out pages at any location.

The electronic version is now web-enabled to allow you to click from web addresses to websites. Please contact the *PL&B* office for more information.

*Privacy Laws & Business has clients in over 45 countries, including the UK Top Ten, eight of the Global Top Ten and seven of Europe's Top Ten in the Financial Times lists; and 10 of the US Top 20 in the Fortune list; and 70% of the top 20 law firms in the London and UK Legal 500 lists.*

# Newsletter Subscription Form

## Subscription Packages

(Please add 17.5% VAT to prices for the PDF format within the EU)

- Print**    **PDF**   (please tick preferred delivery format)
- Send a FREE sample of the *UK/International* newsletter
- PL&B UK* Subscription **£285**
- UK/International* newsletter Combined Subscription **£595** or an extra **£220** for existing International newsletter subscribers
- Special academic rate – 50% discount on above prices

## Multiple Subscription Discounts

- 2-9 copies: 30% discount (indicate no. of copies ....)

## Intranet Enterprise Licence (inc. up to 10 printed copies)

- PL&B UK* **£1,425**
- PL&B International* **£1,875**
- Both *International/UK* newsletters **£2,975**
- I wish to receive *PL&B's* FREE e-mail news service

**Data Protection Notice:** *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you do not wish to be contacted by:    Post    E-mail    Telephone

Name: .....

Position: .....

Organisation: .....

Address: .....

Postcode: ..... Country: .....

Tel: .....

E-mail: .....

Signature: .....

Date: .....

## Payment Options

Address of Accounts (if different): .....

Postcode: .....

- Purchase Order
- Cheque payable to: *Privacy Laws & Business*
- Bank transfer direct to our account:  
*Privacy Laws & Business*, Barclays Bank PLC,  
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.  
Bank sort code: 20-37-16   Account No.: 20240664  
IBAN: GB92 BARC 2037 1620 2406 64   SWIFTBIC: BARCGB22  
*Please send a copy of the transfer order with this form.*

- American Express    MasterCard    Visa

Card Name: .....

Credit Card Number: .....

Expiry Date: .....

Signature: ..... Date: .....

### I am interested in:

- Consultancy/Audits
- In-House Presentations/Training
- Recruitment Service

*Please return to:* Newsletter Subscriptions Department,  
*Privacy Laws & Business*, 2nd Floor, Monument House, 215 Marsh  
Road, Pinner, Middlesex HA5 5NE, UK. Tel: +44 (0)20 8868 9200  
Fax: +44 (0)20 8868 5215   e-mail: [sales@privacylaws.com](mailto:sales@privacylaws.com)  
web: [www.privacylaws.com](http://www.privacylaws.com) 28/11

## [www.privacylaws.com](http://www.privacylaws.com)

## Guarantee

If you are dissatisfied with the newsletter in any way, the unexpired portion of your subscription will be repaid.