pdp JOURNALS

Data Protection Ireland

Volume 5, Issue 5 September/October 2012

Headlines

- ODPC publishes second privacy audit of Facebook, p.17
- Permanent TSB misrepresented credit histories, too p.19
- *FBD v Collins* appeal delayed until 2013, p.20

Contents

DPC pleads poverty as pressure mounts on Ireland

Ireland has been urged by the European Justice Commissioner to prioritise data protection reform during its term of Presidency of the Council of the European Union next year.

Ireland is due to commence its six month Presidency in January 2013, taking over from Cyprus. Speaking during a recent visit to Dublin, Viviane Reding said that, during the time of Ireland's Presidency, the draft Data Protection Regulation "will come to a very crucial, a very sensitive moment."

"As home to many innovative firms dealing with a lot of personal data, Ireland has a key role to play in shaping the new rules," said Mrs Reding.

In response to Mrs Reding's comments, the Data Protection Commissioner, Billy Hawkes, said that data protection authorities will need additional resources to carry out their broader European oversight responsibilities. He said "this is a key issue for us due to the large number of multinational companies handling personal data that have substantial operations in Ireland."

It is not the first occasion that the DPC has called for increased funding for his Office (the ODPC). Launching his Annual Report in April 2012, Mr Hawkes said "Our resources are now stretched to beyond the limit." He also warned that as the ODPC takes on greater responsibility over multinationals which choose Ireland as an EU base, failure to adequately discharge the responsibility of monitoring the companies would "carry significant reputational risks for the country".

(Continued on page 17)

Vodafone pays out €40,000 over unsolicited marketing calls

Vodafone and the Office of the Data Protection Commissioner have concluded agreements to do with the phone company's various breaches of unsolicited marketing rules.

The cases relate to marketing communications made by Vodafone contrary to Regulation 13 of the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011. Vodafone has agreed to make a contribution totalling €40,000 to be shared among a number of Irish registered charities in recognition of the illegal behaviour. The company is also making goodwill gestures to each complainant directly.

Vodfone has put in place additional controls internally and with third party sales agents to ensure that customer preferences are accurately recorded without delay. It has also taken steps to ensure that its agents refrain from engaging in marketing phone calls made for account management purposes to customers who have opted out of marketing contact.

The DPC remains in dialogue with Vodafone as the company enhances its policies and proce-

(Continued on page 17)

Expert comment

Rob Corbet is a Partner at Arthur Cox — the views expressed are his own

On 21st September 2012, the Data Protection Commissioner ('DPC') published his second audit report on Facebook Ireland, following the initial detailed audit report that was published in December 2011.

The initial audit was triggered by specific complaints raised by the 'Europe-v-Facebook' group, the Norwegian Consumer Council and others. The job fell to the DPC due to the fact that Facebook's non-US operations are headquartered in Ireland. Under Section 10(1)(b) of the Data Protection Acts 1988 and 2003 ('the DPAs'), the DPC is obliged to investigate all complaints, unless they are frivolous or vexatious, and to seek to resolve them in the first instance through amicable resolution. (An article on the first audit report was published in Volume 5, Issue 2, of *Data Protection Ireland*).

The second report was the product of the follow-up audit which had been pre-planned as a means of assessing progress made in respect of the implementation of the recommendations in the first report. As with the first audit, the DPC focused on the complaints it was investigating under section 10 of the DPAs, while it also liaised with the Data Protection Supervisory Authorities in other EU Member States to address specific concerns raised by them.

In total, the reports stretch to over 300 pages. So what have we learned?

Lesson 1 — Ireland is a focal point for data protection regulation

As with the first report, the second report attracted global media attention with detailed commentary and analysis appearing instantly, including in the *New York Times* and the *Financial Times*. Given Ireland's positioning as a hub for data centres and 'big data' operators, the integrity and credibility of the reports was important. In this regard, while opinions will differ in relation to the pros and cons of the audit report recommendations, the Office of the Data Protection Commissioner ('ODPC'), is to be commended in producing two comprehensive reports in what must have been trying circumstances.

The broad message from the reports was a positive one in that the ODPC will work constructively with those on the cutting edge of data, while at the same time cooperating with European partners to ensure that genuine privacy concerns are addressed. This is a strong and powerful message to those with existing or potential data operations in Ireland.

Lesson 2 — the ODPC needs more resources

The headlines did not tend to reflect on the fact that the ODPC did not have sufficient internal resources to conduct the audit. With public sector hiring embargos in place, the ODPC had to creatively apply the skills of interns and pro bono technological support to complete its work. In what is hopefully a positive sign on this front, the ODPC has since advertised a new position of 'Technology Adviser', perhaps a sign that the ODPC will be provided with sufficient resources to continue to serve the needs of data subjects and data controllers in Ireland now and into the future. This resource challenge is set to become all the more stark once the draft EU Data Protection Regulation is implemented, at which point the ODPC will be the 'one stop shop' for many multinationals who operate their EU businesses out of Ireland.

Lesson 3 — transparency is in the eye of the beholder

The audits have encouraged Facebook to adopt a more transparent approach to its data management practices. For example, a more prominent privacy policy has been agreed, and more transparency has been introduced to disclose the fact of third party access to data using social plug-ins, especially in the case of any 'friends' apps which grant access to personal data without a person's knowledge.

In keeping with the overarching data protection principle of 'fair processing', the ODPC has also convinced Facebook to provide users with more information so as to enable them to make more informed choices 'inline' or 'just in time' before any use of their data commences. The adoption of a 'welcome dashboard' with enhanced privacy settings will also empower users to adjust their settings to suit their specific preferences at any time.

It would be interesting to know what percentage of Facebook users actually link

through to existing privacy policies and/or change their default privacy settings. Presumably the vast majority of Facebookers will continue to enjoy the benefits of the service without worrying unduly about adjusting their data protection settings, even if they are only vaguely aware that their data are being commercially exploited in the background. However, for the increasing number of new and existing Facebookers who are anxious to guard their privacy, the additional transparency measures will be welcomed.

Lesson 4 — shift towards empowering the customer

The move towards increased transparency is consistent with a shift that is starting to emerge globally. In recent years, many large online operators have realised that hiding away their privacy policies and disguising their data management practices is not a strategy that will ultimately cut the mustard with regulators, nor will it alleviate the concerns of individual customers and privacy advocates. However, there is a disconnect between the ever increasing complexity behind the uses of personal data online (e.g. behavioural advertising, social plug-ins/cookies, etc) and providing individuals with simple and clear choices to manage their preferred privacy standards.

In some cases, an 'ideal' privacy option (as viewed by a privacy regulator) will either eliminate the commerciality of the underlying product and/or severely reduce performance for the user. For companies such as Facebook which are reliant on the commercial application of customised advertising content to turn a profit, this is set to be a perpetual challenge. For consumers, the challenge will be understanding the cause and effect of exercising whatever privacy options are made available to them. In any event, 'Privacy Dashboards', such as those already in use by Google, are likely to become all the more familiar to internet users as a replacement to the bewildering number of privacy-related FAQs which users currently face when they seek to understand or adjust their privacy settings.

Lesson 5 — facial recognition is a red flag issue

Facebook's 1 billion users upload 300 million images a day. While that does not in itself present a data protection 'no no', the photo tagging feature introduced by Facebook overstepped the mark. The ODPC determined that there was no compelling case as to why Facebook members cannot exercise their right to prevent their image being tagged, notwithstanding the potential loss of control and prior notification that may come with that choice.

Interestingly, the tagging feature appears to have been an issue where the ODPC felt that Facebook had gone further than was strictly necessary under Irish law. The second report notes that the feature has been removed to assuage the concerns of supervisory authorities in other jurisdictions. Perhaps there is a hint here that the ODPC was less exercised about the issue than its equivalent bodies elsewhere. In any event, Facebook has disabled the feature for now. Given the technological developments that are ongoing in the area of biometrics and facial recognition, this is likely to be an issue that will emerge again.

Lesson 6 — the right to be erased

The ODPC has insisted upon 'fully verified' account deletion at the end of the customer life cycle. In addition, Facebook is required to improve the information provided to users in relation to what happens to deleted or removed content (e.g. friend requests, received pokes, removed groups and tags, deleted posts, etc). Users should also be able to delete friend requests, pokes, tags, posts and messages, and "so far as is reasonably possible delete on a per item basis". These recommendations reflect the underlying data protection rule not to retain personal data for longer than necessary, a very challenging rule to implement for a company of Facebook's scale. However, it is interesting to note that the ODPC acknowledges the practical challenges associated with removing data, and this provides Facebook with an ability to implement changes without necessarily restructuring huge parts of its service.

Lesson 7 — privacy by design is here already

Judging by the audit reports, the proposed introduction of 'Privacy by Design' under the draft Regulation is here already. Facebook has agreed with the ODPC that it will put in place a more comprehensive mechanism, "resourced as appropriate", for ensuring that the introduction of new products or uses of user data take full account of Irish data protection law. In so doing, Facebook has agreed that it will consult with the ODPC during the process of improving and enhancing existing initiatives prior to their implementation.

Any comments or feedback on this or other items covered in *Data Protection Ireland* are always welcome by the editorial team.

I am delighted to say that I will be once again chairing the Annual Data Protection Practical Compliance Conference, which will take place in Dublin on 22nd and 23rd November 2012. See www.pdp.ie/conference/ for further details.

Rob Corbet
Partner at Arthur Cox
rob.corbet@arthurcox.com

Data protection and employment — Part 5

Oisin Tobin and Philip Nolan, from Mason Hayes & Curran, discuss the data protection issues involved in disclosure of employee data during due diligence processes in the context of mergers and acquisitions

The purchase of a business can be a complex process. The buyer needs to develop a deep understanding of the company that it intends to acquire to ensure that it represents a sound investment, and is worth the price sought. This detailed knowledge is usually acquired through an analysis of all aspects of the target's operations. This analysis process, usually termed 'due diligence', may involve the disclosure of personal data, including the data of employees.

This article considers the data protection issues involved in disclosure of employee data during the due diligence process. We will also look the ways that data protection law can impact upon mergers and acquisitions ('M&A') activities in other ways, for example, issues that arise with respect to the transfer of customer databases (particularly in cases where only parts of the business are being sold via an asset sale) and the data protection assurances (or warranties) given by the seller.

How do the issues arise — a scenario

The best way to consider the issues arising during a due diligence process is by way of an example:

Target Co is an Irish based SME with 150 employees. Buyer Co is an international conglomerate headquartered in New York. Buyer Co wishes to acquire the entire issued share capital of Target Co. Before the sale can complete, Buyer Co wishes to acquire detailed information about, among other things, Target Co's employees, including union activities and absenteeism.

Addressing this example requires consideration of a number of different data protection issues:

- is the transfer of employee data to Buyer Co a data controller to data processor transfer, or a data controller to data controller transfer?
- what conditions must be met before Target Co can transfer employee personal data to Buyer Co?
- can Target Co transfer employees' sensitive personal data to Buyer Co?
- what restrictions should be placed on Buyer Co's use of the employee information?
- do the employees need to be notified about the transfer?
- can the employee data be transferred to the US?

How should we classify this disclosure?

The rules governing data controller to data controller transfers differ from the rules governing data controller to data processor transfers. Thus it is important to establish at the outset whether Buyer Co is receiving the employee personal data as a data controller or a data processor.

Section 1 of the Data Protection Acts 1988 and 2003 ('the DPAs') define a data controller as being 'a person who, either alone or with others, controls the contents and use of personal data'. In contrast, a data processor is defined as 'a person who processes personal data on behalf of a data controller'. In the above example, Target Co is handing over information about its employees so as to enable Buyer Co, and its advisors, to consider the risks involved in the transaction, to draft the deal documentation properly and to properly assess the value of Target Co. In a context such as this, it is clear that Buyer Co receives the employee personal data on its own behalf, and for its own purposes. In these circumstances Buyer Co is a data controller in respect of the employee data transferred as part of the diligence process.

Pre-conditions to transfer

The handover of employee personal data from Target Co to Buyer Co is a form of processing and, consequently, is only permissible if one of the pre-conditions set down in Section 2A of the DPAs has been met.

The two key pre-conditions in the above context are 'consent' and 'legitimate interests'. Section 2A(1)(a) allows for processing in circumstances where the employee has freely given his or her

specific and informed consent. A well drafted employee privacy policy should contain a provision which foresees the handover of personal data as part of a merger, acquisition or restructuring. The Data Protection Commissioner ('DPC') has endorsed this approach in his guidance note 'Transfer of Ownership of a Business' (available at www.pdp.ie/docs/10004) ('Guidance note'), which states that: '[S]uch an eventuality should be foreseen in an organisation's Data Protection Policy. The policy should provide that certain specifiable personal data may be disclosed in the context of acquisition discussions, particularly because secrecy may be a condition of negotiations.'

If the relevant employee privacy policy does not contain a robustly drafted clause allowing for the disclosure of personal data in the event of a corporate deal, then it should ideally be amended and redistributed.

As regards the conditions in section 2A(1)(a), it is, of course, open to Target Co to seek the relevant consents from its employees during the deal process. This approach may work if, for example, Target Co is a small enterprise (such as a family owned business). However, seeking such consents, mid-deal, could prove to be extremely difficult for medium or large businesses.

If employees have not consented to the transfer, Target Co may be able to rely on its legitimate interests, or those of Buyer Co, to legitimise the transfer. Section 2A(1)(d) of the DPAs allows for processing, in the absence of consent, where it is necessary 'for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed'. This justification is not available if the processing causes unwarranted prejudice to the fundamental rights and freedoms or interests of the relevant employees.

"In light of the above, the best practice approach would be to remove any specific medical or union information relating to an identifiable employee from material handed over to Buyer Co. Though information with respect to levels of abstinence, or union membership may be provided, it should be given in an anonymised or aggregate form."

The transfer of information so as to conduct a proper diligence of Target Co would appear to be in the legitimate interests of Buyer Co, and also possibly Target Co. In his Guidance note, the DPC accepted the availability of the legitimate interests justification in an M&A context. If the parties intend to rely on this justification, it is particularly important that proper safeguards are put in place to protect the employees' personal data. If such safeguards are not put in place, there is a possibility that the processing may cause 'unwarranted prejudice' to the employees, negating this justification.

Disclosure of sensitive personal data

Section 1 of the DPAs defines sensitive personal data as including (amongst other things) data relating to health or union membership.

The disclosure of this information as part of the diligence process can be problematic. A buyer may be interested in obtaining this information, so as to assess the level of employee abstinence or to consider the possibility of industrial unrest. However, from the perspective of data protection law, such information cannot be handed over unless at least one of the conditions in Section 2B of the DPAs is met. One cannot rely on general consent, or legitimate interests, to handover this information. In his Guidance note, the DPC suggests that sensitive personal data can rarely be handed over as part of a diligence exercise:

'Disclosure of sensitive data, such as individual employees' health data or union membership details, should be avoided unless one of the provisions of Section 2B of the Acts can be relied upon which is unlikely in most acquisition processes.'

If Target Co wanted to hand over sensitive personal data, it would likely need to show that it had obtained the explicit consent of the employee or, alternatively, that the employee had deliberately made the relevant information public.

Thus it may be theoretically possible to disclose medical or trade union information if an employee explicitly agreed to such disclosure. However, the employer would need to show that such consent was freely given. In the employment context, this could be a challenge. Alternatively, if an employee had deliberately and publically disclosed the relevant information (such as if they announced that they were a shop steward in a publication), then the information may be handed over.

In light of the above, the best practice approach would be to remove any specific medical or union information relating to an identifiable employee from material handed over to Buyer Co. Though information with respect to levels of abstinence, or union membership may be provided, it should be given in an anonymised or aggregate form.

Protecting employee interests

In the above example, Target Co should limit the extent to which Buyer Co can process the employee data. This is not only commercially advisable, but may also be necessary to

(Continued on page 6)

(Continued from page 5)

ensure that Target Co is meeting its obligation to keep the personal data secure (under Section 2(1)(d) of the DPAs) and to avoid unnecessary processing (Section 2(1)(c)(ii)).

In his Guidance Note, the DPC advises that Target Co should only hand over personal information prior to the final merger or acquisition decision after securing formal assurances that:

- it will be used solely for the evaluation of assets and liabilities;
- it will be treated in confidence and will not be disclosed to other parties; and
- it will be destroyed or returned after use.

In a practical sense, these assurances should be given in the confidentiality agreement which should be signed at the start of the deal process.

Fair processing

As noted above, the handover of employee personal data from Target Co to Buyer Co constitutes a data controller to data controller transfer. The fair processing obligations as set down in Section 2D of the DPAs require that employees be informed of this transfer. This notice should ideally be given before the transfer of the relevant personal data. On a literal reading of Section 2D, this notification should come from Buyer Co. However, in practice, this notification is often given by Target Co, since it has the relationship with the employees.

This notice should at least detail the name of Buyer Co and the categories of personal data being transferred, and make it clear that personal data are being transferred in connection with the proposed transaction.

Data transfer

In the above example, Buyer Co is based in New York. Consequently, part of the diligence exercise may be conducted by its executives, or advisors, in the US. This will require that the employee personal data be transferred outside of the European Economic Area. Section 11 of the DPAs prevents such a transfer in the absence of certain pre-conditions being met. In a M&A context, the key pre-conditions are employee consent, Safe Harbor and the use of EU Commission approved Model Clauses.

Ideally, the employees will have consented to the transfer of their personal data. If such consent has not been provided and the transfer is to a US based Buyer Co, it may be worth checking if Buyer Co participates in the US Department of Commerce Safe Harbor scheme. If there is no consent to the transfer, and Safe Harbor is not an option, it may prove necessary to put a data controller to data controller model form agreement in place between Target Co and Buyer Co so as to legitimise the export of the personal data.

Conclusion

The sale of a business can be a challenging but exciting time for any organisation and its employees. Numerous issues need to be considered, and addressed, to bring the deal to a successful conclusion. In the midst of this activity, it is important not to forget employees' data protection rights. Simple forward planning, particularly with respect to the preparation of an organisation's privacy policy, can go a long way towards heading off these issues.

Philip Nolan and
Oisin Tobin
Mason Hayes & Curran
pnolan@mhc.ie
otobin@mhc.ie

Challenging times ahead for data processors

Bridget Treacy, Partner at Hunton & Williams, ***discusses the obligations on data processors as set out in the draft Data Protection Regulation, including the challenges for processors presented by the Regulation as currently drafted***

Much has already been written on the proposed EU Data Protection Regulation, but there has been very little focus on the fundamental changes to the responsibilities and liabilities that the Regulation seeks to impose on data processors.

Currently, a processor has no direct responsibility or liability under the Data Protection Directive (although processors do have direct obligations under Irish implementing legislation); the new Regulation introduces a raft of direct obligations and subjects processors to the same enforcement mechanisms as a data controller, including the possibility of substantial administrative fines of up to 2 to 4% of their worldwide turnover.

The essence of a processor's role

Determining whether a party is a 'processor' or a 'controller' is a fundamental distinction in European data protection law, not least because the Directive imposes direct responsibility (and liability) on a controller, not on a processor. The controller will usually allocate responsibility to a processor as a matter of contract.

Whether a party is a controller or processor can be a difficult assessment, frequently involving fine distinctions. In February 2010, the Article 29 Working Party published a widely anticipated 'Opinion on the Concepts of Controller and Processor' (www.pdp.ie/docs/10008). The Opinion's focus is on the role of the controller in ensuring data protection and therefore much of it is devoted to explaining how to determine controllership. The Working Party characterises the role of the processor as subsidiary to that of a controller, and emphasises that the existence of a processor is wholly dependant on a decision taken by a controller to delegate data processing activities to a third party. Thus, a processor needs to be a separate legal entity, and to undertake data processing activities on behalf of another, the controller. The Opinion is clear that whether or not a party is a processor is fact specific and depends on 'concrete activities in a specific context'.

Given the level of debate over the years as to the roles and responsibilities of a data controller versus a data processor, there was speculation that, in reforming data protection law, EU law-makers might remove the distinction altogether and instead impose responsibility on parties for the data processing activities they conduct. This has happened in many of the jurisdictions that form the Asia-Pacific Economic Cooperation. However, the current draft of the Regulation does not do this. Instead, it seeks to require the parties to establish the limits of their authority and authorisation, and to adhere to them.

Obligations imposed on processors

Chapter IV of the draft Regulation sets out the obligations imposed on both controllers and processors. Article 26 sets out the specific requirements where a controller seeks to delegate processing to a processor. These requirements, which must be imposed contractually, are similar to, but extend beyond, what is currently required under the Directive. Unsurprisingly, a key focus is on data security and a controller must chose a processor that provides sufficient guarantees to implement appropriate technical and organisational measures and procedures.

However, the security objective is expanded with the requirement that guarantees must be given 'in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'. This amendment apparently seeks to ensure that processors are able to deliver compliance across a broader range of rights, which are set out in further detail in Article 26(2). Yet the role of a processor is different to that of a controller and clearly there are aspects of the Regulation that processors cannot generally be expected to comply with. This provision is just one of several in which the role and responsibility of the processor require further consideration.

(Continued on page 8)

(Continued from page 7)

Contractual requirements

Article 26 also sets out requirements that must be reflected in the contract between the controller and processor. These are more extensive that those currently required by the Directive.

There is a subtle difference between the wording of the draft Regulation and the Directive on the subject of whether a contract need be entered into between a controller and processor. The Regulation states (at Article 26(2)) that "*the carrying out of processing by a processor* shall be governed by a contract" (italics added); this can be contrasted with the requirement under the Directive that all data controllers must put in place processing contracts with their 'data processors'.

The significance of this distinction becomes apparent when you consider that processors can be penalised directly by data protection authorities for failure to comply with Article 26. The administrative sanctions in Article 79(6) impose the highest level of fine (up to 2% of annual worldwide turnover) for breach of the provision. These fines may be imposed on those who carry out processing, which includes the processor. Specifically, Article 79(6) permits the imposition of a fine not just on a controller but on anyone who, intentionally or negligently 'processes…personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26…'. Therefore, a processor could be subject to a sanction of the highest level if the controller fails to enter into a contract with it.

"There are many hundreds of thousands of services agreements and outsourcing contracts in the EU, most of which are unlikely to comply with the enhanced contractual requirements set out in the Regulation. Renegotiating such contracts to ensure compliance would take a lengthy period, certainly longer than the two year implementation period envisaged for the Regulation generally."

The specific requirements listed in Article 26 require that the processor will:

- act only on the instructions of the controller, in particular where the transfer of personal data used is prohibited;
- employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
- take all measures required in relation to the security of processing, as set out in Article 30;
- enlist another processor only with the prior permission of the controller;
- create, in agreement with the controller, the necessary technical and organisational requirements to enable the controller to comply with individuals rights set out in Chapter III (which deal with transparency, information, rights of access, rectification, the right to be forgotten, erasure, portability, the right to object and profiling);
- assist the controller in complying with Articles 30 to 34 (which deal with data breach notification, data protection impact assessments ('DPIAs') and prior authorisation);
- hand over results at the end of processing and not to process data otherwise; and
- make available to the controller and supervisory authority all information necessary to control compliance with the obligations laid down in Article 26 (see further below).

In addition, the controller and processor must document the controller's instructions and processor's obligations. If the processor processes personal data other than as instructed, the processor shall be considered a controller and subject to the rules on joint controllers, set out in Article 24.

Article 24 simply provides that where a controller determines the purposes, conditions and means of the processing jointly with others, the joint controllers shall determine their respective responsibilities for compliance under the Regulation. Thus, if a controller failed to give proper processing instructions, Article 26(4) may have the effect of transforming a processor into a controller. This may also occur where a processor inadvertently processes personal data, for example, because the processor does not realise that data contain personal data elements. It seems difficult to imagine that these consequences were intended.

The meaning of the last subsection of Article 26(2)(h), which refers to making available 'all information necessary to control compliance', is unclear. It appears to extend far beyond a general obligation to provide information, which sits awkwardly with the separate obligations in the Regulation that require the parties to maintain documentation recording processing operations, and permitting the supervisory authority to require information.

Overall, the Regulation envisages very detailed contractual provisions which would create a significant additional burden in many cases. A number of the issues listed in Article 26 are issues that will be covered by due diligence investigations between the parties in most cases, but which seem inappropriate as detailed contractual terms. Further, where data processing arrangements are com-

plex, the relevant level of specificity may not be available at the time the contract is entered into, so that these provisions will need to be supplemented as the contract evolves.

At a practical level, the Regulation does not address the position of existing contracts, or make specific arrangements for transition. There are many hundreds of thousands of services agreements and outsourcing contracts in the EU, most of which are unlikely to comply with the enhanced contractual requirements set out in the Regulation.

Renegotiating such contracts to ensure compliance would take a lengthy period, certainly longer than the two year implementation period envisaged for the Regulation generally. Further, as inevitably happens, once an agreement is re-opened, one or other of the parties will invariably seek to negotiate other terms; a process which could be very expensive for organisations. It is hoped that, at the very least, existing contracts will remain valid until the data processing activities changed, at which point new provisions could be negotiated.

"As a general observation, the Regulation does not clearly set out which provisions are applicable to controllers, which apply to processors, and which apply to both. The position is confused because some obligations are not attributed to either controller or processor, some are attributed to the controller, but then the supervisory authority can serve notices in respect of them on the processor, and others are referred to as being exercised by the processor 'on behalf of' the controller."

Maintain documentation

Both controllers and processors are obliged to maintain documentation of all processing operations for which they are responsible (Article 28(1)). In particular, the Regulation sets out the following minimum requirements:

- name and contact details of the controller/joint controller/processor/representative;
- name and contact details of the Data Protection Officer ('DPO');
- purposes of the processing (including the legitimate interests pursued by the controller, where the processing is based on legitimate interests);
- description of categories of data subjects and categories of personal data relating to them;
- recipients or categories of recipients of the personal data;
- transfers of data to a third country or international organisation;
- general indication of the time limits for erasure of different categories of data; and
- description of the mechanisms referred to in Article 22(3), namely, the mechanisms that the controller uses to verify compliance with its obligations set out at Articles 22(1) and (2). In particular, these include documentation required under Article 28, data security requirements (Article 30)), DPIAs (Article 33), prior authorisation/prior consultations with supervisory authorities (Article 34) and designated DPO (Article 35).

There is also a general obligation on both the controller and processor to make the documentation available on request to the supervisory authority. There is an exemption to complying with this obligation for organisations with fewer than 250 employees whose data processing activities are ancillary to its main activities, and for natural persons processing data without a commercial interest.

A key difficulty here is that much of the information listed in Article 28(2) will be commercial information of the controller, not the processor, yet the obligation to maintain the information rests with both parties. Further, supervisory authorities may impose a fine of up to 1% of an enterprise's annual worldwide turnover where it intentionally or negligently fails sufficiently to maintain the documentation required by Article 28.

Processors' obligations unclear

The key obligations under the Regulation — i.e. the 'principles relating to personal data processing' listed in Article 5 — are clearly responsibilities of a controller. The grounds for processing (Articles 6 —10) also make clear that any basis for processing must be attributed to the data controller and not to the processor. The obligations of transparency (Articles 11—13) are imposed on the controller alone. The rights to information, access to data, rectification and erasure and other individual rights (Articles 14 — 21) are only exercisable against the controller. Yet, processors (as well as controllers and representatives, if any) are required to cooperate with the supervisory authority (Article 29(1)), in particular, in connection with alleged breaches of the Regulation reported to the supervisory authority and the exercise of data subject rights.

Both processors and controllers are obliged to reply to requests of the supervisory authority relating to the exercise of data subjects' rights within a 'reasonable period' (to be specified

(Continued on page 10)

(Continued from page 9)

by the supervisory authority) (Article 29(2)).

Thus, as a general observation, the Regulation does not clearly set out which provisions are applicable to controllers, which apply to processors, and which apply to both. The position is confused because some obligations are not attributed to either controller or processor, some are attributed to the controller, but then the supervisory authority can serve notices in respect of them on the processor, and others are referred to as being exercised by the processor 'on behalf of' the controller. Clarity around which responsibilities are attributable to the processor would assist.

An example of this confusion may be seen in the context of subject access. Supervisory authorities may serve notices on processors where controllers fail to provide subject access. Yet none of the individual rights are exercisable directly against the processor, and the processor can have no liability for failing to comply with them. Allowing the supervisory authority to proceed against a processor may be appropriate as a secondary remedy where the controller has been required to deal with an access request but has failed to do so properly, but the processor should not be the primary recipient of such a notice.

Processor as joint controller

The provisions on joint controllership set out in Articles 24 and 26(4) do not sit well together. Article 24 contains the following wording: 'where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers…'. This implies that 'joint controllers' are controllers where two (or more) controllers jointly decide the purposes, conditions and means of the data processing. Further, joint controllers must determine their respective responsibilities for compliance with the Regulation by means of an arrangement between them.

This should be contrasted with the position of a processor which exceeds its authority or strays into controllership. Article 26(4) provides that 'if a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.' Here, the processor is not a 'joint controller' with the original controller, because the two have not decided the purposes, conditions and means of the data processing together. Nevertheless, Article 26(4) provides that the processor-turned-controller would be subject to the Article 24 requirement to allocate controllership responsibilities with the original controller.

Taken together, Articles 24 and 26(4) appear to mean that a processor which carries out relatively minor processing outside the scope of its instructions becomes subject to the obligations of a joint controller under Article 24. The outcome has unintended consequences as, presumably, the processor-turned-controller may approach the original controller and demand that the original controller agree with it the exercise of their 'respective responsibilities'. It may give unscrupulous processors a basis to put pressure on controllers by acting outside their remit. In most cases, this would be a breach of contract and it is not at all clear how a regulator would be able to enforce something that amounted to a contractual breach by the processor.

Conclusion

The Regulation is ambitious, seeking to implement wide-ranging reform across many aspects of data protection law. Some themes are relatively self-contained, but others, such as the role of the data processor, are nuanced and complex. It is only with careful reading and analysis of the proposed Regulation that the significance of the changes proposed for data processors becomes apparent.

The responsibilities and liabilities of processors will change fundamentally if the current proposal is enacted. Many processors will not have focused on these issues yet. It is to be hoped that they do so soon.

Bridget Treacy
Partner
Hunton & Williams
btreacy@hunton.com

Data Protection Impact Assessments: look before you leap

Stephanie Pritchett, Solicitor and Principal of Pritchetts, explains what would be required to comply with the draft Data Protection Regulation's requirements on mandatory Data Protection Impact Assessments

Most readers will be aware that the European Commission published its proposed new Data Protection Regulation ('draft Regulation') on 25th January 2012. Once it has been approved by both the European Parliament and the European Council, the draft Regulation will replace the current Data Protection Directive (95/46/EC) and will amount to extensive revision of data protection legislation across the European Union. Whilst approval is not currently expected to happen until 2014, it would be prudent for many organisations to start tweaking their data protection policies and procedures now, in anticipation of both the more extensive compliance responsibilities and the potential new increased fines of up to 2% of annual worldwide turnover, a sizable stick in anyone's language.

Introduction of mandatory 'Data Protection Impact Assessments'

Amongst the various new requirements set out in the draft Regulation, Article 33 introduces the need for data controllers and data processors to carry out mandatory 'Data Protection Impact Assessments' ('DPIAs') before carrying out high-risk data processing activities. These assessments are not a new concept — 'privacy impact assessments', as they were previously known, have been around for some time. It is the legal obligation to carry out such assessments in certain circumstances that is the new element.

When will we have to carry out Data Protection Impact Assessments?

Under Article 33(1) of the draft Regulation, where data processing operations 'present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes', the data controller, or the data processor acting on its behalf, will be required to carry out a DPIA to consider what the impact of the proposed processing operations will be on the protection of personal data.

The circumstances requiring a DPIA to be carried out under Article 33(1) are relatively vague and will require a certain amount of subjective consideration by organisations. However, Article 33(2) sets out some of the circumstances which will definitely be considered to present the requisite risks. As a result, there will be no question about the need to carry out DPIAs where the following processing activities are proposed:

- a systematic and extensive evaluation of personal aspects relating to a natural person, or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;
- information on sex life, health, race and ethnic origin, or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for the purpose of taking measures or decisions regarding specific individuals on a large scale;
- monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale, e.g. CCTV systems;
- personal data in large scale filing systems concerning children, genetic data or biometric data;
- any processing operations which data protection authorities ultimately designate as being likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes. Authorities will have this right under Article 34(2)(b) of the draft Regulation provided that they establish and make public a list of any processing operations where a DPIA and/or consultation with the authority will be necessary; and
- any processing operations

(Continued on page 12)

(Continued from page 11)

which the European Commission ultimately designates as presenting specific risks to the rights and freedoms of data subjects. The European Commission will have this right under Article 33(6), subject to certain procedures being followed.

The requirements to carry out DPIAs will be relaxed a little for public bodies or authorities that are carrying out processing activities as a result of a European Union legal obligation. In those situations, relevant national organisations will not be required to carry out DPIAs unless national law requires that it is necessary for them to do so in particular situations (Article 33(5)).

Readers may be interested to note that, during the interservice consultation period, further requirements to carry out DPIAs in routine circumstances where employee data are to be processed were actually removed from the draft Regulation. This removal reduced what could have been a very onerous burden on most employer organisations to a collective sigh of relief from industry.

"However, it remains to be seen whether authorities will have the time or resources to be able to give organisations the comfort they need to continue with riskier processing operations, particularly in the timely fashion which may be needed for urgent projects. This will certainly be the case should authorities become inundated with consultation requests, which there is currently a high risk of in the proposed new regime."

How will we carry out Data Protection Impact Assessments?

Article 35 of the draft Regulation will require all organisations of more than 250 employees, and all public authorities, to designate a Data Protection Officer ('DPO'). It is likely that one of the key roles of these DPOs will be to carry out DPIAs, as well as any necessary consultation with the relevant regulator.

The key elements of the new obligation to carry out DPIAs will be as follows:

Provision of certain information: The DPIA will need to set out (under Article 33(3)): a general description of the envisaged data processing operations; an assessment of the risks to the rights and freedoms of data subjects; and the measures proposed to address the risks as well as the intended safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the draft Regulation, having taken into account the rights and legitimate interests of data subjects and other persons concerned.

Seeking views of data subjects: Data controllers will be required to seek the views of relevant data subjects (or their representatives) on the impact of the intended new processing, without prejudice to the protection of commercial or public interests or the security of the processing operations (Article 33(4)).

Policies and procedures: Data controllers will need to put in place policies and procedures to ensure workers know how to carry out DPIAs (Article 22).

Delegation to processors in certain circumstances: Data controllers will in some circumstances be allowed to delegate responsibility to data processors under the draft Regulation. This may include both the need to carry out a DPIA or to consult with the data protection authority before starting to process information in riskier ways. This new ability to delegate responsibility will make it very important for data controllers and data processors to set out contractually:

- a clear division of any such responsibilities; and
- appropriate warranties and indemnities to ensure that if a breach does occur as a result of inadequate DPIAs or consultation, it is clear who will accept financial liability and responsibility for the breach.

This contractual division of responsibilities may be particularly important, as it is currently unclear from the draft Regulation which party the relevant data protection authority would pursue by way of monetary penalties and other sanctions when any such non-compliance occurs.

Powers of the European Commission: under Articles 33(6) and (7), the European Commission will be able to specify certain standards, procedures or requirements that will have to be followed by data controllers or data processors carrying out, verifying and/or auditing DPIAs. This includes conditions for scalability, verification and auditability.

It seems likely that we will see more information produced in due course in relation to how organisations will be expected to conduct DPIAs and what they should contain. The draft Regulation states that in producing these standards, the Commission will have to consider specific measures for micro, small and medium-sized enterprises.

Organisations will no doubt be hoping that any additional requirements

imposed by the Commission will be drafted proportionately, having taken into account the likely size and resources of particular organisations. This is so particularly given the Commission's estimates that DPIAs can range in cost from €14,000 for a small-scale assessment, €34,500 for a medium-scale assessment, and up to €149,000 for a large-scale assessment.

What happens if the DPIA concludes that there is a high level of data protection risk involved in carrying out intended processing operations?

Interestingly, organisations will be required to consult their national data protection authority in respect of any proposed processing which may be considered to present 'specific risks' following the conclusion of the DPIA (Article 34).

Given the potential new fines of up to 2% of annual worldwide turnover for non-compliance, the fact that Article 33 is very broadly drafted, and with the onward reporting requirement under Article 34, it is likely that many organisations may well choose to carry out DPIAs and self-report to authorities in the hopes that the authority will 'sign-off' on projects following that consultation, thereby minimising risks of sanctions being applied.

However, it remains to be seen whether authorities will have the time or resources to be able to give organisations the comfort they need to continue with riskier processing operations, particularly in the timely fashion which may be needed for urgent projects. This will certainly be the case should authorities become inundated with consultation requests, of which there is currently a high risk in the proposed new regime.

Perhaps national authorities will produce guidance about the situations where they are likely to engage in consultation (e.g. where there are more chances of 'serious breach' or damage being caused to individuals).

Are DPIAs a good idea?

The introduction of mandatory DPIAs will force organisations to carry out a greater level of data protection due diligence before undertaking riskier data processing activities. Crucially, this work will only be effective if organisations carry out reasonable risk analysis assessments to ensure 'privacy by design' and where meaningful reports are produced, as opposed to organisations simply completing a bureaucratic box ticking exercise (or sub-contracting this work to data processors without proper consideration).

DPIAs should be used by all organisations designing and upgrading new data processing systems and procedures to help ensure privacy and data protection risks are considered at early stages in projects. This can only minimise the risks of breaches occurring further into project timetables and becoming costlier and more resource intensive to deal with.

It is hoped that organisations will not be mandated to only use DPIAs in situations where 'riskier activities' are being carried out, but that they will instead be encouraged to either use DPIAs (or the national authority's equivalent) for other, perhaps less risky, data processing projects.

Conclusion

We may see a dual system evolve, whereby mandatory DPIAs will need to be carried out in 'riskier' situations, (yet to be fully defined by the European Commission), but where national regulators will still encourage the use of PIAs in other circumstances.

Whatever the position with PIAs, organisations will undoubtedly have to build more time into project timescales to carry out mandatory DPIAs both in order to ensure privacy compliance and risk mitigation and also to consult national authorities where that becomes necessary. This will certainly create a greater administrative burden as well as adding to the implementation costs of many new projects.

Ultimately the payoff could be substantial: tighter compliance, investor and board confidence, good PR and a lower risk of expensive and damaging regulator intervention. Let's all look a bit more closely before we leap.

Stephanie Pritchett
Pritchetts Law
stephanie@pritchettslaw.com

The new rules on using children's data

Anita Bapat, Associate at Hunton & Williams, describes the major changes to processing of children's data as required under the proposed EU Regulation

The draft Regulation on the processing of personal data ('the draft Regulation') places restrictions on the use of children's data. This contrasts with the current regime under Directive 95/46/EC, which contains no specific rules on the use of children's data. The draft Regulation carves out specific considerations to be taken into account when processing children's personal data, for example in the context of the fair processing of information and the right to be forgotten. Somewhat controversially, the draft Regulation defines a child as "any person below the age of 18".

Parent/guardian consent for children under 13

Article 8(1) of the draft Regulation makes it unlawful to process the personal data of a child under 13 in the context of offering information society services, without the consent of a parent or guardian. An information society service, as defined in Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC, is 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'. Such a definition potentially has very wide application and would, most likely, apply to almost any form of commercial website. Further, according to Article 8(2) of the draft Regulation, a data controller should ensure that consent is verifiable, taking into account available technology.

There are several practical difficulties inherent in obtaining parental consent or authorisation for the processing of children's data when providing them with information society services. These are detailed below:

How parental consent will be obtained is not clear: If mechanisms such as inputting of a parent's email address or date of birth are used to obtain consent, children would be able to circumvent such measures easily, for example by inserting an incorrect date of birth or using an email address which is their own rather than their parent's.

When consent should be obtained is not prescribed: For example, would parental consent for a child using a social networking site be required when a child under 13 signs up for an account or every time the child interacts with the site?

It is challenging for a data controller to obtain parental consent that is verifiable: There is no guidance in the draft Regulation as to what 'verifiable' means, except that available technology will be taken into account. Obtaining consent that is verifiable, whilst preferable, is a challenging threshold to satisfy in practice. This is especially the case where a child could easily use a fake email address to circumvent parental consent, as stated above.

The provisions apply to any information society service, irrespective of the risks involved, which seems unduly restrictive: For example, some online activities such as games or quizzes have minimal risk to privacy, if any.

Such a requirement does not take into account circumstances where children under 13 may want to access services without parental consent: For example, children may wish to use a confidential support line. This point was made by the UK regulator in its initial analysis of the Regulation. The Information Commissioner's Office ('ICO') recommend such circumstances be taken into account given the invaluable service they provide to society.

Right to be forgotten

Article 17 of the draft Regulation provides for the 'right to be forgotten'. This is the right of an individual to request erasure of personal data, especially data made available by the individual when he or she was a child, when such data are no longer necessary for the purposes for which they were collected or the individual withdraws consent to the processing. The specific reference to data collected when the individual was a child is significant: Article 17 is a right that targets the use of social networking and other sites which are predominantly used by children. There has been a lot of press attention and public concern expressed over personal information about individuals when

they were young re-emerging and individuals having no recourse to remove such information. The inclusion of this right, therefore, acknowledges the permanency of data once put online and seeks to alleviate concerns by providing a mechanism for its removal.

Article 17 does not apply to the retention of criminal conviction data as such matters will be covered by the draft Directive on police and criminal justice data. However, it does acknowledge the undue detriment that may be caused to individuals as a result of retention of data.

Fair processing information

Under Article 11(2) of the draft Regulation, a data controller must provide information relating to the processing of personal data to the individual in an intelligible form, and use clear and plain language adapted to the individual, particularly when the information is addressed to a child.

Whilst the right of subject access under the draft Regulation essentially follows the current Directive, the requirement to ensure that the language is adapted to the individual and in particular to children, is significant. This establishes the fair processing of information as a subjective right and places a clear onus on a controller to provide information that is transparent and tailored to an individual.

The specific reference to children is an example of the safeguarding of children's rights over their personal data and seeks to ensure that they are informed of, and genuinely understand, the nature of data processing activities (even if parental consent is required under Article 8 (1)).

Conclusion

The specific references to children in the draft Regulation are a welcome step in implementing safeguards on the use of children's personal data. Such safeguards seek to protect children's participation in online activities as well as the processing of their data more generally. The considerations to be taken into account are not particularly innovative and should be what any data controller processing children's personal data is doing currently. Nonetheless, they serve to emphasise the special nature of children's personal data.

However, some view the provisions in the draft Regulation relating to children as imposing impractical restrictions on the use of children's data. In particular, the requirement to obtain parental consent for the processing of personal data of a child under 13 would appear challenging. Many see the imposition of this requirement without any guidance as to how this is to be achieved to be a missed opportunity in providing a practical solution for obtaining genuine parental consent for their children's activities. Therefore, while the provisions in the draft Regulation are welcomed, further guidance from the European Commission as to how the provisions can be satisfied in practice would be useful.

Anita Bapat
Hunton & Williams
abapat@hunton.com

News & Views

Ireland a key player in reform

(continued from page 1)

The Irish regulator's ongoing audit of Facebook (see news item below) appears to have been met with approval by other DPAs and the European Justice Commissioner, who commended the regulator's work whilst she was in Dublin. However, the audit is understood to have placed a considerable burden on the ODPC.

The decision of whether to award the ODPC with additional resources is one for the Irish government, which is currently understood to be examining the case. The DPC has a staff of 22, seven of whom are Investigating Officers and three are Compliance Officers. By way of comparison, France has a total staff of over 140 and Germany just under 100 on federal level, as well as at least another hundred dispersed across its 16 landes. The UK Information Commissioner's Office has a total staff of 350.

Meanwhile, the Civil Liberties, Justice and Home Affairs Committee has discussed the planned timetable for adoption of the Regulation. A vote on the Regulation is expected to take place between February and April 2013, to enable negotiation with the European Council later on. The overall plan is to have the content of the Regulation agreed in 2014.

Vodafone settlement

(continued from page 1)

dures to ensure full compliance with its data protection obligations with regard to marketing communications.

ODPC concludes second privacy audit of Facebook

The Irish regulator has published the results of its second privacy audit of Facebook.

The follow up audit was carried out in order to assess how far recommendations from the first audit have been implemented by the social network.

The ODPC concluded that it is satisfied with the great majority of steps that Facebook has taken to follow best practice recommendations. The report said that transparency, user control over settings, clarity over retention periods, and user access rights have all improved. In areas where progress has not been as fast as hoped, for example better education for current users, the ODPC set a deadline of four weeks for implementing recommendations.

There was one aspect of the audit in which the social network exceeded expectations of the ODPC and other regulators — Facebook voluntarily switched off its facial recognition service in Europe. Although not part of the its initial recommendations, the ODPC had requested during the course of 2012 that Facebook turn off its tag suggest feature for all new users. It is understood that the ODPC, not being too concerned about the feature itself, made the request as a concession to other European privacy regulators. The company went beyond the ODPC's request by saying it would switch the feature off altogether (i.e. for existing users also) by 15th October 2012. The company says it wants to reinstate the feature once a form of consent can be found that meets the guidelines.

The news of Facebook's suspension of its facial recognition feature met with approval elsewhere in Europe: Hamburg Commissioner for Data Protection and Freedom of Information, Johannes Caspar, said "We are happy that the Irish Data Protection Commissioner could achieve this", adding that this is more than what he asked for.

Deputy Commissioner, Gary Davis, said that Facebook still needs to be monitored going forward, especially since the social network is constantly adding features to its service.

A copy of the audit report is available at www.pdp.ie/docs/10005

Meanwhile, two US privacy watchdogs filed a joint letter with the Federal Trade Commission alleging that Facebook may already be flouting an agreement to be provide greater clarity over how it handles user data. According to the Center for Digital Democracy and the Electronic Privacy Information Center, Facebook's partnership with a data collector called Datalogix may violate parts of a recent FTC consent order that outlined privacy principles Facebook should follow. The FTC's determination is awaited.

Meteor and eMobile spared convictions

Two of Ireland major phone companies which were the subject of the first prosecutions for loss of personal data on unencrypted laptops, have escaped conviction.

Meteor and eMobile admitted breaking data protection laws in early September 2012, following investigation by the

(Continued on page 18)

(Continued from page 17)

Irish regulator into the theft of two laptops which contained sensitive personal information about thousands of customers. The court had ordered both companies to donate €15,000 to two charities. However, during follow up proceedings, a judge ordered each company to donate €15,000 to charities nominated by him, but applied the Probation Act in lieu of convictions because they had pleaded guilty and neither company had prior convictions from breaching data protection laws.

A spokesperson for the ODPC told *Data Protection Ireland* "[the prosecutions] send a strong message to the companies involved, other companies in the telecommunications sector and indeed data controllers more broadly, that failing to comply with security requirements will have consequences in terms of reputation and the bottom line. The prosecutions also make clear that failing to report data breaches to this Office and affected individuals in a timely manner is not acceptable and may lead to action by this Office."

The spokesperson added: "the exact manner of how the Court wished to sanction Eircom and Meteor is not a matter for this Office."

Shatter to revisit Privacy Bill over topless Kate

The Irish government is to revisit privacy regulation in the country following the Irish *Daily Star's* publication of topless photos of the Duchess of Cambridge.

In a strongly worded statement, Justice Minister Alan Shatter said he was going to return to Ireland's 2006 Privacy Bill to "consider what changes should be made" and then "progress its enactment". He added that despite the existence of a press regulator, "some sections of the print media are either unable or unwilling in their reportage to distinguish between 'prurient interest' and 'the public interest'".

Dr Eoin O'Dell, Associate Professor at Trinity College Dublin, commented: "in practice such a law would become a vehicle simply for the rich and powerful, politicians, businessmen, bankers and footballers, secretly to muzzle press investigation. It is a blunt, disproportionate and unnecessary response to the *Star's* peeping tom images which can be dealt with by other means. The Minister should think again."

EU cloud partnership to be established

The European Commission has unveiled a new strategy document for cloud computing, revealing a plan for cloud computing to generate 2.5 million new jobs by 2020, and boost GDP by €160bn a year.

The document reveals that the Commission will launch three cloud-specific actions: cutting through the 'jungle of standards', establishing safe and fair contract terms and conditions, and establishing a European Cloud Partnership (ECP) to drive innovation and growth from the public sector. The ECP, which is being established this year, will provide an umbrella for comparable initiatives at Member State level. The ECP will bring together industry expertise and public sector users to work on common procurement requirements for cloud computing in an open and fully transparent way.

The Commission will report its progress on the actions in the strategy document by the end of 2013, and present further policy and legislative proposal initiatives as needed.

A copy of 'Unleashing the potential of cloud computing in Europe' is available at www.pdp.ie/docs/10006

EDPS calls for standard security requirements for electronic ID schemes

The European Data Protection Supervisor, Peter Hustinx, has said that third party organisations tasked with certifying that systems individuals use for inputting personally identifying information are genuine should have to abide by a 'common set of security requirements.'

The EDPS, whose official role is to monitor data protection compliance within EU institutions and bodies, recommended that the single set of data security standards should be detailed under the EU's proposed Electronic Trust Services Regulation, or else a provision should be put in place to allow the European Commission to "define where needed, through a selective use of delegated acts or implementing measures, the criteria, conditions and requirements for security in electronic trust services and identification schemes."

The European Commission proposed the draft Electronic Trust Services Regulation in June 2012 in a bid to make it easier and more secure to complete e-commerce transactions across the EU without complication.

A copy of the EDPS's Opinion is available at www.pdp.ie/docs/10007

Uruguay achieves adequacy in data protection

Uruguay has been declared 'adequate' by the European Union for the purposes of foreign data transfers. The country is the tenth (after Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man and Jersey) to be recognised by the Commission as having an adequate level of protection for personal data.

The Principality of Monaco is likely to be next to receive adequacy status from the Commission following the Article 29 Working Party's Opinion that the Principality ensures an 'adequate level of protection' for personal data within the meaning of the European Data Protection Directive.

Data Protection Essential Knowledge — Levels 1 & 2

These two practical training courses taken together constitute a complete training package on the fundamentals of data protection.

Level 1 is an invaluable introductory (or refresher) level training course, conducted by Peter Carey, a dually

qualified Irish and UK solicitor, and author of *Data Protection: A Practical Guide to Irish and EU law.* Level 2 covers essential data protection topics not covered in he Level 1 session..

The next three dates for the sessions are:

Level 1:

- Dublin — Monday, 12th November 2012
- Cork — Monday, 25th February 2013
- Dublin — Tuesday, 26th February 2013

Level 2:

- Dublin — Tuesday, 13th November 2012
- Cork — Tuesday, 26th February 2013
- Dublin — Wednesday, 27th February 2013

Further 2013 dates are available. For further information, or to make a booking, visit www.pdp.ie/training

Permanent TSB misrepresented credit histories, too

Following the news report in the previous edition of this journal ('Country's banks under investigation'), Billy Hawkes has urged Irish bank customers to check their credit records after discovering that misreporting of clients credit histories to the Irish Credit Bureau has taken place elsewhere than Allied Irish Bank.

AIB was discovered to have been sending incorrect statements to the Irish Credit Bureau detailing missed loan repayments relating to about 12,000 customers over a six-year period up to July 2012. This prompted the Office of the Data Protection Commissioner to carry out audits of banks and other financial institutions to see whether the practice was widespread.

The audit has yet to be completed, but the DPC said that a similar problem had been found in at least one other financial institution, Permanent TSB.

Swiss watchdog in row about workers' privacy

Switzerland's Data Protection Commissioner has demanded that Swiss banks cease the practice of handing over information to the US authorities that reveal the identities of staff.

In April 2012, the Swiss government authorised some banks to transfer records after the US threatened to open criminal proceedings against them. The data were supposed to be encoded to protect the identity of individuals, but it has since come to light that key information has been pieced together to reveal the names of client advisors and other bank employees.

Hanspeter Thür only knew of the government's April decision when "numerous" bank employees started to contact his office. The watchdog subsequently wrote to several banks, the Swiss Bankers Association and the Swiss Private Bankers Association to set out the restrictions of handing over information according to Swiss law. "We have informed them that we are opening an analysis to verify the legality of the data transmitted to the US," Thür said. "Until we have the results, we have demanded that no further bank employee data be sent to the US."

The banks have agreed to inform employees in detail before transferring data to foreign tax investigators. Five banks signed agreements to notify employees.

Though the Swiss DPA acts mainly in an advisory and dispute settlement role, it also has enough teeth to haul miscreants that flout data protection laws before the courts. Last year, the watchdog won a court ruling that compelled Google to protect the privacy of individuals visible in its Street View application. The Federal Court lifted some restrictions of that decision in June 2012, but the combined rulings were widely seen as a victory for the Swiss Commissioner.

New data protection law imminent in Singapore

A proposed Personal Data Protection Bill in Singapore has received its first reading in the country's Parliament.

The Bill proposes a framework-based, rather than prescriptive, type of regulation. Organisations will therefore be required to devise their own practices and policies around data protection that meet its requirements.

One key provision in the Bill is the new section covering the transfer of data outside Singapore. The new Section 26 provides that an organisation is not permitted to transfer data outside Singapore "except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data". Compliance falls upon the sending organisation to ensure a comparable (with the Singapore Act) level of protection in the receiving organisation.

The new Bill would also establish a new Personal Data Protection Commission, with powers to fine businesses up to SIN$100,000 (approximately €63,000) for obstructing its performance of duties.

Row erupts over asylum seekers database

A row between the European Commission and the European Data Protection Supervisor has broken out over plans to give police access to biometric data from the fingerprints of asylum seekers.

The controversy centres on the role of EURODAC, the EU-wide fingerprint database. The database was originally created in 2000 to prevent multiple claims for asylum being lodged in different Member States, with no country taking responsibility for the application. The establishment of the database

(Continued on page 20)

(Continued from page 19)

was accompanied by specific safeguards that data are not used for other purposes.

In May 2012, the Commission adopted a proposal concerning a recast of the EURODAC Regulation, allowing national law enforcement authorities and the European police service, Europol, to access the EURODAC central database for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences. The change would have the result that, if a fingerprint is found at a crime scene, asylum seekers could potentially be identified through EURODAC data while other individuals could not because of a lack of availability of similar data on all other groups of society.

In his 20 page report, Peter Hustinx accused the European Commission of failing to provide sufficient evidence and justification for the plans, stating that the Commission should prepare a fresh impact assessment "in which solid evidence and reliable statistics are provided and which includes a fundamental rights assessment."

A spokesperson for Home Affairs Commissioner, Cecilia Malmström, said "we welcome the report of the EDPS and will consider it thoroughly in the context of the pending negotiations with Council and the European Parliament."

FBD v Collins appeal delayed until 2013

A significant appeal on the courts' ability to award compensation for damages to individuals that have had their rights under the Data Protections Acts 1988 and 2003 breached has been delayed until next year.

The appeal is bring brought by FBD Insurance following the Irish Circuit Court's decision in March 2012 to award an individual compensation in relation to FBD's various breaches of data protection law. The breaches included failure to have in place a written contract with a contractor (data processor) and failure to appropriately handle an access request. The insurance company's customer, Michael Collins, was awarded €15,000 in damages under section 7 of the DPAs. The appeal hearing was due to be heard on 5th October 2012.

Mr Collin's lawyer, Fintan Lawlor, of Lawlor Partners, told *Data Protection Ireland* "it is unfortunate that, due to a large backlog of cases, the High Court is currently not in a position to rule on this matter. The question of damages remains open in relation to data protection breaches, with the Circuit Court award of €15,000 the sole case we can currently refer to.

"Until the matter has been decided by the High Court we remain uncertain as to what sum the courts will deem adequate for compensating a breach of data protection."

pdp JOURNALS

Data Protection Ireland

EDITOR: Rezzan Huseyin

EDITORIAL BOARD MEMBERS:

Rob Corbet, Partner — Arthur Cox
Paul Lavery, Partner—McCann Fitzgerald
Annette Orange, Partner—McCann Fitzgerald
Catrin Prys-Williams, Legal Manager—Accenture
Peter Carey, Consultant—Charles Russell
Colin Rooney, Partner—Arthur Cox

SUBSCRIPTIONS MANAGER: James Anderson

SUBSCRIPTION ENQUIRIES:

Ireland: +353 (0) 1 657 1479
United States: +1 (615) 469 4594
Email: journals@pdp.ie
Website: www.pdp.ie/journal

Back issues and electronic version available on request