ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

‘Battle tested’ Denham ready to take reins at the ICO

Laura Linkomies reports from Parliament in Westminster on the appointment that now awaits the signature of the Queen.

Elizabeth Denham, currently Information and Privacy Commissioner in British Columbia, Canada, was confirmed as the next UK Information Commissioner by the House of Commons Department of Culture, Media and Sport (DCMS) Select Committee on 28 April after interviewing her the previous afternoon.

“I’m battle tested as a Commissioner,” she said. “I have never shrunk away from an important issue. I cross swords with the largest tech companies – I led the first investigation into Facebook – no other

Continued on p.3

Get GDPR ready and update your privacy policy now

As the ICO nudges companies to begin GDPR preparations, **Lore Leitner** and **Calum Docherty** look at the privacy policy options.

A recent study found that 38% of Americans are confused by privacy policies.[1] This is not surprising. Many Internet users and customers find the information provided in privacy policies notoriously impenetrable, and, at times, Delphic. Often, these policies are drafted – by lawyers – with a view to protect companies rather than to enlighten their users.

As we wrote in last September’s issue of *PL&B UK Report*, September 2015 pp. 7-8), the General Data Protection Regulation (GDPR), which was adopted last month after

Continued on p.4

Issue 85 **May 2016**

UNITED KINGDOM
report

ISSUE NO 85 MAY 2016

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

SUB EDITOR
Tom Cooper

REPORT SUBSCRIPTIONS
Glenn Daif-Burns
glenn.daif-burns@privacylaws.com

CONTRIBUTORS

Lore Leitner & Calum Docherty
Latham & Watkins LLP

Merrill Dresner
PL&B Correspondent

Michael D. Smith
Reed Smith LLP

Dugie Standeford
PL&B Correspondent

William Long & Francesca Blythe
Sidley Austin LLP

Nicola Fulford & Gemma Lockyer
Kemp Little LLP

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

Next steps for data protection in the UK

Now that we have the EU Data Protection Regulation, the next thing to look out for is UK implementation, which is expected to be – again – different from most EU Member States. The derogations obviously give all Member States some leeway (p.10) but it is more than likely that the UK government will continue its business-friendly manner of regulating data protection. Watch out for any announcements of a new data protection law or other type of UK regulation in the Queen's Speech on 18 May.

Whatever happens, the new EU regime will create much more work for the ICO, to be headed after 28 June by Elizabeth Denham, currently Information and Privacy Commissioner, British Columbia, Canada. We at *Privacy Laws & Business* are fortunate to have had a great working relationship with her for many years and look forward to seeing how she will apply her Canadian experience in the UK (p.1).

The ICO is preparing guidance on the GDPR. In the meantime, read what our contributors say about revising privacy policies for the GDPR era (p.1), and how to start a successful GDPR compliance programme (p.20). In the public sector, changes to the legitimate interest ground for processing are causing extra concern (p.8).

Our management stories in this issue include a report on the experience of the Royal Mail (p.13) and Transport for London (p.18). Also, read on p.16 about the new world of Artificial Intelligence and consequential challenges to data protection concepts.

The Data Retention and Investigatory Powers Act 2013 (DRIPA) is due to expire in December 2016, and the government is therefore in a hurry to adopt the Investigatory Powers Bill. Having visited Westminster to attend Elizabeth Denham's hearing before the Department of Culture, Media and Sport Select Committee, and having listened to the joint committee and the three witnesses on the human rights aspects of the Bill, I must say that it sounds to me that the issues are still far from clear. The experts basically concluded that the Bill does not include proper human rights protections. The main issue is about proportionality. But a European court case may soon challenge the legality of UK's surveillance laws anyway (http://bit.ly/1SZEfLx). In the meantime, the Open Rights Group has published an informative comparison of changes between the first and current version of the Bill (http://bit.ly/1TPx88Z).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Elizabeth Denham ... from p.1

DPA had gone there. I knocked on their door in 2008 when they had a mere 300 million users. This was a small office in Canada investigating Facebook. The same with Google when I served at the Federal office – I started an investigation into Google StreetView because they were hoovering up unsecured WiFi data that had been illegally collected by the company when they were collecting StreetView images. That was a serious investigation that took us down to Google's lab so that we could witness the destruction, the deletion, of the Canadian data. I think we might have been the only Data Protection Authority that followed through to make sure that collected data was properly and securely deleted." In 2008, Facebook had no privacy controls, Denham explained, but its response after the investigation was to put controls in place worldwide. Both companies are now more careful with data and have a different infrastructure, and carry out a dialogue with DPAs. But these big companies are becoming monopolies and we need to watch them, she said.

Denham comes into the role with an impressive privacy career already behind her. Since 2010 she has been the Information and Privacy Commissioner for British Columbia, Canada, responsible for enforcing the Canadian Freedom of Information and Protection of Privacy Act (FIPPA), the Personal Information Protection Act (PIPA), and the Lobbyists Registration Act (LRA). Previously (2007–10), she was the Assistant Privacy Commissioner at the federal level. Denham will start in her new position as soon as possible after Christopher Graham's term of office ends on 28 June. This is the first time that *PL&B* is aware that any Data Protection or Freedom of Information Commissioner anywhere has been appointed from a different country.

Ready to fine bad actors

A pre-appointment hearing by the Parliamentary Committee on 27 April had a potential veto over the appointment, and spent one and quarter hours asking wide-ranging questions including how she would make the transition from Information and Privacy Commissioner for British Columbia (BC), to becoming the UK Information Commissioner.

"The Information Commissioner in the United Kingdom has similar powers to the powers that I have as a Commissioner in British Columbia, so I have order-making power; I have quasi-judicial decision making in freedom of information that is appealable to the courts on an error in law, on judicial review, so that is very, very similar. When it comes to data protection though, I would say Canada has softer laws. The Privacy Commissioners in Canada do not have the civil monetary penalties and powers that exist for the Information Commissioner on the data protection side in the United Kingdom."

Denham explained that Canada has 30 years of experience of Freedom of Information law compared with 10 years in the UK. As a result of her investigations, the BC government had responded in a serious way making substantial changes.

Denham said that she would be willing to impose large fines on companies when 'things go very wrong,' citing the maximum fine of 4% of annual global revenue included as a sanction in the EU Data Protection Regulation. "Data protection is the responsibility of directors to take it out of the IT department and into the board room," she said.

However, she said that her approach as the UK Information Commissioner would be firstly to educate and advise organisations and conduct audits. She said that sometimes it is the smaller companies that pose the biggest challenge as for them, reputational impact is not as important as for household brands. Currently, smaller companies that receive fines in the UK sometimes go into liquidation to avoid paying, and then start again with another name. Denham suggested that company directors should be made personally liable for data breaches in some situations. "Sanctions for bad actors are necessary and healthy for a digital economy." Denham said however that she would continue the approach she had in Canada of engaging with stakeholders, including companies, in order to be informed of what they are planning next.

FOI aspects

The MPs were particularly interested in hearing how Denham would deal with government communications under the FOIA. Referring to use of private e-mails and social media for official public sector communications, she explained that her guiding principle is that "it is the message not the medium" that is important. "Even private emails can be caught under FOIA," she said. "There should be a duty to document serious decisions."

She suggested that government, the civil service, and MPs should use only government communication networks, and use two separate mobile phones – one for business and another one for private matters.

She said she supports extending FOIA to not-for-profit organisations and companies carrying out work for public sector bodies. She said that proactive disclosures cut down the number of FOI requests, and should therefore be encouraged.

Denham has conducted some high-level FOI investigations in Canada, resulting for example in the Access Denied report (*PL&B UK* November 2015 pp.14-16).

"The Access Denied report was an examination of two government ministries and the Office of the Premier. My office investigated because a whistleblower came forward with serious allegations that senior staff were triple-deleting records and deleting records that were potentially responsive to freedom of information requests. Those were very serious allegations. I had written three reports prior to that investigation where I found practices that were not respectful of freedom of information. Those were gentler reports. In the last report, we found some very, very serious contraventions of the law. We interviewed people for the first time under oath. We removed computers and did forensic examinations. Unfortunately, one of the ministerial aides misled my staff under oath and I turned that file over to a special prosecutor that has now charged that individual. That was a very serious investigation."

She said that Section 77 of the UK's FOIA has provisions that would enable similar action in the UK. "But regular audits are a better way forward."

ICO MANAGEMENT STRUCTURE

Denham was asked how she would deal with heading a very large office of more than 400 staff. She responded by saying that at the federal level, she was responsible for 100 staff. She said that the ICO was an important office "which casts a long shadow around the world. It is a tech-savvy practical office that I think fits with my outlook on data protection and freedom of information." She said she would first have to rely on her staff to be briefed on some UK-specific issues, such as the Talk Talk breach or the Motorman inquiry.

"I will have some studying to do to understand the UK environment but I am a fast learner."

She said that the future challenge within the ICO is the change in management. She thought that more senior posts will have to be created. The ICO has been forward thinking under Richard Thomas and Christopher Graham, and she has had the pleasure of working with both of them, and other ICO senior staff in international fora. She said she would visit the three ICO regional offices within the first 30 days of her taking office.

"I think that I have been a strong leader and a manager and I have been successful in managing budgets, always coming in between 95% and 99%. I have been successful in recruiting excellent staff, building teams and I think that the Information Commissioner requires the same skillset. You have a strategic plan, you make sure that your direct reports understand and the rest of the organisation understands the vision, you check back with the staff, you review their work. I think feedback is really important and face-to-face bilateral meetings are very important."

Denham was asked: Would you work for the Government or Parliament?" In a firm declaration of principle, she responded: "For Parliament and the people."

She said that the structure here was different from Canada in that in British Columbia, she reports to the legislature. Whilst the UK ICO is completely independent, it has to work with a government department, the DCMS.

EU GDPR PROSPECTS

Denham said she understood that the UK might opt for a more business-friendly route via some of the exemptions available under the EU General Data Protection Regulation (GDPR). But the Regulation will form an adequacy standard to which other countries, including Canada which currently has an adequacy decision, will have to work towards.

She thought that one of her first jobs would be to resolve the ICO's future funding issue. The abolition of notification fees will see the ICO's funding cut by 80%. Future work will concentrate on preparing guidance on the GDPR, but at the same time, the office needs to continue to manage complaints and deal with its other existing responsibilities.

The GDPR will introduce a breach notification duty. Denham said on audit powers: "The audit power of the Information Commissioner is a patchwork right now, so there are not compulsory audits for all types of organisations. I think Christopher Graham made the point to this Committee that compulsory audit powers would be very helpful to him in this role. I have a preliminary view on that, but again, I need to understand the issues and I need to get my feet under the table to be able to comment on that question."

She thought, however, that as local authorities have much sensitive data, an audit power would be a useful tool in that area.

OTHER CHALLENGES

When asked if she had the determination to deal with a potentially hostile media, she told the committee that she had conducted around 100 interviews last year with the media and civil society organisations in BC which are "very engaged" and "not gentle".

She thought that the Investigatory Powers Bill would create "a honey pot of data which would have to be very secure." But there is no such thing as perfect security, she said.

The MPs were keen to hear how she would handle nuisance calls. She said that she understood the DCMS had already introduced some increased protections such as calling line identification. She was keen to carry on this work: "It is a complex problem as well, because there is a legitimate business in direct marketing, so again, what you are trying to do is take the bad actors out of the situation and protect the legitimate calls." She said that the DPAs Global Privacy Enforcement Network was of great help in these kind of cases when they have an international dimension.

INFORMATION

See the select committee document at http://bit.ly/1QV0ka0 and
Written evidence at http://bit.ly/1TuTc5H

GDPR ... from p.1

over four years of debate, attempts to redress this imbalance by putting data subjects' informed choice at the forefront. In addition, consent will be the cornerstone of this new regime: a data subject's consent must be "freely given, specific, informed and unambiguous" and data controllers must be able to demonstrate this consent. The GDPR is clear that "silence, pre-ticked boxes or inactivity should not therefore constitute consent" and that "when the processing has multiple purposes, consent should be given for all of them".

For many data controllers, privacy policies are the gateway to data subject consent. As this consent becomes more difficult to validly attain under the GDPR, privacy policies will have to change both in terms of content and format. Data controllers will have to think carefully to navigate the potential tension between Article 13's increased consent requirements and Article 12's emphasis on simplified formats.

Article 13 of the GDPR has set out new minimum requirements for what needs to be provided in privacy policies: a data controller must now inform data subjects of:

1. its identity and contact details and (where applicable) those of its representative;
2. the contact details of its data protection officer (where applicable);
3. the purposes of the processing for which the personal data are intended

as well as the legal basis for the processing;
4. the legitimate interests pursued by the controller or by a third party (where applicable);
5. the recipients or categories of recipients of the personal data (if any); and
6. the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or specify where they have been made available (where applicable).

In addition, if such information is necessary to ensure fair and transparent processing, the data controller must also specify:

7. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
8. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
9. where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
10. the right to lodge a complaint with a supervisory authority;
11. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and
12. the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

While this long list may require a thoughtful internal audit to make sure a privacy policy adequately reflects a company's privacy practices, these content requirements are not likely to impose an excessive burden on data controllers. In our opinion, most data controllers will err on the side of caution and include more rather than less information to ensure they meet the requirements set forth in the GDPR. Hence, Article 13 of the GDPR may just make privacy policies (even) longer, and even less likely to be read by data subjects.

Yet Article 12 provides that communications from data controllers to data subjects should be "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". This is easier said than done. Along with the study mentioned above, CNN reported last year that users would need to be educated to at least the level of a second-year university student to understand the disclaimers in the privacy policies of several large online businesses, and an oft-cited Carnegie Mellon study from 2008 estimated that it would take the average person 76 working days to read all of the privacy policies he or she encounters in a year.

So what is to be done? It is unsurprisingly difficult for data controllers to distil complex technical practices into clear consumer-facing communications – yet data subjects must understand what happens to their data in order to validly give consent to processing. This is particularly important as non-compliance can result in hefty fines of up to 20 million euros or 4% of global turnover, whichever is greater. The old approach of bombarding users with dense legalese is unlikely to satisfy the consent conditions of the user-focused GDPR, and more innovative formats are required to engage and inform data subjects, so that their consent can be validly given. This article will outline some potential solutions for data controllers seeking to write better privacy policies, first in terms of formats and then in terms of practical tips.

Formats

To achieve a better level of compliance under the GDPR, data controllers will need to make more of an effort to engage with their users. We looked at some of the UK Information Commissioner's Office (ICO) new proposals and other solutions which are discussed in the industry, to give you an overview of approaches which may be suitable under the GDPR.

1. Layered notices: A layered approach is not new. For a long time, it has been recommended by the ICO as best practice. Layered notices can simplify complex information by highlighting the salient points of the privacy policy up front. At the top level, there could be a clear and succinct summary of the information required under the GDPR. Users would then have the option of clicking through the summary into more detail on a particular point of interest (for instance, to click through to a detailed section on data transfers). This approach allows the user to have a high-level understanding of the key issues (and grant consent thereto), but also enables the user to delve deeper at his or her own volition. It is important however that the high-level summary reflects a data controller's practices accurately (and does not oversimplify important practices) or else consent may not be deemed to be valid.

The layered approach will become particularly relevant in a mobile context, as often mobile screens allow for less space to display privacy information. Therefore, data controllers will need to experiment with click-through tabs and interactive messages to get their privacy messages across.

2. "Just in Time" notices: Instead of relying on consent from a "one size fits all" privacy policy, data controllers should consider providing "just in time" notices at critical data processing junctures. These notices work by appearing on the individual's screen at the point where he or she inputs personal data, providing a brief message explaining how the information about to be provided will be used. This will enable users to have an informed understanding of how their data will be processed. For instance, if a user's date of birth is requested to sign up for a service, a "just in time" notice should explain why this information is needed and how it will be processed. This could work by generating pop-up bubbles if a user hovers his or her mouse over a text input box, for example, so the user's consent is more specific to

the actual processing of particular data categories. As such, these "just in time" notices more effectively allow data controllers to demonstrate that consent was validly given by a data subject. On the other hand, providing notice – and obtaining consent – in this way does have a risk of restricting the data controller in its future use of data if it has not specified each purpose of processing in each "just in time" notice.

3. Icons and symbols: The GDPR empowers the Commission to provide standardised icons and to develop procedures for implementing such icons. The icons are intended to give data subjects a "meaningful overview of the intended processing" in "an easily visible, intelligible and clearly legible manner." The key to such icons is that users will quickly understand what the data controller will do with their personal information – yet the icons must themselves be intuitive. Many data controllers have voiced concern in this regard, and do not wish to see any icons which are unclear or too detailed and unwieldy to include in privacy policies of limited length, for example, on mobile screens. While the Commission refines its approach, different data controllers may want to consider using and/or proposing graphics to better engage their data subjects and to set the standard.

4. Interactive approaches – videos: User expectations are evolving. Rather than passively reading a text-heavy policy, users may prefer to engage directly by watching online videos. This approach has seen a marked upswing in popularity, with sites such as Google, the Guardian and Channel 4 creating comprehensive videos to highlight the information collected from data subjects and how this data is used. These short videos can provide compelling content through both visuals and audio. Moreover, by creating a script to follow, a data controller can ensure that information is clearly presented – if an actor says something aloud that is overly complex or legalese, lines can be revised to better communicate to data subjects.

5. Privacy dashboards: Data controllers can also consider using privacy preference tools to empower users to manage their own consents, which should be freely given and which users should be able to withdraw at any time. This approach is a helpful one-stop consent shop for users. It can help data controllers by clearly breaking down the purpose of the data processing activity, its legal basis and other factors so users can make informed judgments as to consent. However, problems could arise where a data controller relies on other grounds for processing (such as legitimate interests) and this could lead to users feeling somewhat disempowered as they will not be allowed to make a choice in relation to such purposes of processing. At any rate, privacy dashboards allow users to elect to consent or withdraw their consent at any time for each processing activity, which promotes the undergirding purpose of the GDPR: to focus on data subjects.

Practical tips

The GDPR will enter into force in the first half of 2018, but data controllers would be wise to update their privacy policies now to ensure compliance and to promote clear communications with their customers. The ICO is also weighing in on the matter – it emphasised the importance of communicating privacy information in its March 2016 publication Preparing for the GDPR: 12 Steps to Take Now[2] and it has recently wrapped up a consultation on privacy policies and communicating data protection information to individuals.

In the meantime, data controllers should consider the following:

- **Audit data protection practices:** First and foremost, information provided to data subjects must be accurate, so that data subjects can make informed choices about uses of their personal data. A data protection audit will help businesses understand how and why data is processed, and enable them to explain such practices clearly to consumers. The GDPR requires that consent should be acquired for each data processing purpose, so organisations should clearly break these down and seek consent for each.
- **Use new formats:** Once the audit is complete, data controllers should consider using a new format to more effectively communicate information to individuals. A dense, jargon-laden policy is unlikely to meet the requirements of the GDPR and, at any rate, is not within the spirit of the Regulation. The choice of format will obviously be very product and sector specific.
- **Work with the communications team:** For larger organisations especially, privacy policies should not be isolated within the legal or compliance functions. It would benefit consumers if data protection officers were to work with members of an internal communications or public relations team to craft clear messages for data subjects, without losing any substance. This skills synthesis could clarify information practices to users and allow them to give valid consent to data processing.
- **Test the privacy policy:** Before launching the privacy policy, data controllers should consider testing it with a focus group of users. Honest feedback on the policy will ensure that communications to data subjects are appropriate, and could aid a data controller in meeting its compliance obligations.

AUTHORS

Lore Leitner is an Associate, and Calum Docherty a Trainee Solicitor at Latham & Watkins LLP, London.
Emails: Lore.leitner@lw.com
calum.docherty@lw.com

REFERENCES

1 http://www.pewresearch.org/fact-tank/2015/12/30/americans-conflicted-about-sharing-personal-information-with-companies/
2 https://dpreformdotorgdotuk.files.wordpress.com/2016/03/preparing-for-the-gdpr-12-steps.pdf

Do employers have the right to read employees' private emails?

The *Barbulescu* case has been misinterpreted by many. **Michael D. Smith** explains what the decision means for companies.

A recent European Court of Human Rights (ECHR) case (*Barbulescu v Romania*)[1] has attracted much publicity in the UK press as giving employers the green light to read employees' private emails. Is that correct and does this case really change things?

Barbulescu was employed as an engineer in charge of sales. His employer had a strict policy of not permitting private use by employees of its computer and telecommunications systems. Barbulescu was asked by his employer to set up a Yahoo Messenger account so that Barbulescu could communicate with customers.

Sometime later, the employer notified Barbulescu that it had been monitoring his account and they believed that he had been using it for private communications. Barbulescu denied this at which point his employer presented him with a 45-page transcript of all his Yahoo Messenger communications, including private communications with his fiancée and brother. Barbulescu was dismissed for breaching the employer's policy on personal use of computer systems.

Barbulescu subsequently brought employment claims in the Romanian courts alleging that his dismissal was void since the employer had breached his right to privacy by accessing his private communications. He was unsuccessful before the Romanian courts but his case was brought before the European Court of Human Rights. Mr Barbulescu's argument was that Romania had failed to protect properly his Article 8 right to respect for his private and family life, his home and correspondence.

The ECHR's Decision

The first key point made by the ECHR was confirmation that Article 8 is engaged to protect employees who use their employer's telecommunications systems for private purposes. In other words, employees have a reasonable expectation of privacy at work. Nonetheless, this right is not absolute. The question in this case was whether Romania had struck the right balance between protecting the right of Mr Barbulescu to privacy at work with that of his employer to manage its resources effectively.

The ECHR found against Mr Barbulescu in this regard. It noted that:

- the employer had a clear policy regarding the private use of the employer's telecommunications systems;
- it had not been unreasonable for the employer to want to verify that its employees were engaged on professional tasks during working hours;
- monitoring was the only effective way of ensuring that telecommunications were being used for work-related purposes;
- when the employer accessed the Yahoo Messenger account, it did so in the belief that the account contained only employment-related messages, this being the basis on which the account had been set up; and
- the employer had not gone beyond examining the Yahoo Messenger account to checking any other documents or data on his computer.

Therefore, the employer's monitoring was limited in scope and proportionate.

What does this mean for employers in the UK?

Contrary to some of the more lurid headlines in the press, this case does not give employers carte blanche to read their employees' private emails. In fact, it reiterates principles that have long applied in the UK, namely that employees do have a right of privacy at work but, notwithstanding that, employers do have the right in limited circumstances to monitor private communications at work. The ECHR's judgment is a reminder that any monitoring must be done in a limited manner and proportionately to the issues involved.

If monitoring is to take place:

- Make sure that this is clearly stated in a policy that is brought to the attention of all affected employees. The policy should state which communications may be monitored and in what circumstances. This will set the expectations of employees as to the circumstances in which their communications may be monitored.
- Limit the number of individuals within your organisation who may undertake monitoring and set out clear ground rules about the monitoring that can take place which are consistent with company policy.
- Ask yourself whether monitoring is really required in a particular situation.
- Act proportionately – if your concern is, for example, the volume of private emails being sent, it is usually not necessary to read the contents of those emails to establish the point.

AUTHOR

Michael D. Smith is Counsel at Reed Smith LLP.
Email: msmith@reedsmith.com

REFERENCES

1 www.scribd.com/doc/295296174/Barbulescu-Romania

BARBULESCU CASE: NO REAL CHANGE UNDER UK LAW

Stewart Room, Partner at PWC states that the *Barbulescu* decision has not really changed anything for the UK.

He said that at the moment, the UK DP Act means that organisations should notify employees and third parties of any monitoring, have a proper justification, apply controls and safeguards, and consider the ICO's Employment Practices Code.

However, consent is not needed.

Under the Interception Regulation of the Investigatory Powers Act 2000 (RIPA) and Lawful Business Practice Regulations 2000, which apply to interception, interception on public networks may be a criminal offence. However, interception on a private network is permitted if conducted by the systems owner, and is conducted for a statutory purpose. The employer has to warn employees, but consent is not needed.

Legitimate interest ground under the GDPR:Change ahead

The new EU Data Protection Regulation does not provide for a legitimate interest exemption for public sector data processing. **Dugie Standeford** looks at the implications.

The EU General Data Protection Regulation (GDPR) may now be finalised, but questions about how it will work in practice are far from settled. One murky area concerns whether public bodies can ever rely on the legitimate interest exception to process personal data.

"It's a big question" because of the Freedom of Information (FOI) Act, said Rosemary Jay, senior consultant attorney at Hunton & Williams. Unlike the Data Protection Directive, the GDPR expressly bars public authorities from relying on a legitimate interest when processing data "in the performance of their tasks." The regulation's recitals note that, "Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks."

Public authorities have either legal obligations (duties), such as emptying bins, or discretionary powers to do things they're not required to do, such as building flood defences, Jay said in an interview. Local authorities' discretionary powers have grown much broader in order to ensure they are not unduly constrained from acting in the public interest, she said.

Given that, it would seem evident that under the data protection regime, public bodies seeking to process personal data would look either to the legal duty or public interest exception, Jay said. The GDPR now explicitly removes the latter from consideration, but the UK Information Rights Tribunal over the years has held that when public authorities seek to disclose data as a result of FOI requests, they must rely on legitimate interest rather than legal duty, and balance the duty to disclose with fairness to the data subject. This raises the question of how the UK will deal with the GDPR legitimate interest exception in relation to FOI requests, Jay said.

> The Regulation does not envisage scrapping the legitimate interests basis for essentially private activities of public authorities.

"Business as Usual"

Under the current data protection regime, a public authority that is required to release personal data under FOI should apply the data protection principles, said Amberhawk Training Limited Director Sue Cullen, but in the context of FOI disclosures it's the first principle that counts – that the processing be fair and lawful – together with Schedule 2 and Schedule 3 in cases of sensitive personal data.

Lawfulness is normally not an issue in FOI, Cullen said; all the hundreds of FOI cases fought over through the years come down to the questions of whether disclosure is fair to the data subject and whether it can be justified under Schedule 2[1], conditions relevant for purposes of the first principle processing of any personal data. Condition 5 requires that the processing be necessary for the exercise of functions conferred on an organisation by statute, but from early days, the justification for disclosures by public authorities has always been Condition 6 (legitimate interests pursued by the data controller or by the third party to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason or prejudice to the rights and freedoms or legitimate interests of the data subject). Although the tribunal and the courts have applied Condition 6 for the past 10 years, there was always the argument that the appropriate condition should have been Condition 5, Cullen said, because that is the condition intended for use by public authorities. Condition 6 is now GDPR Article 6 (1) (f), which is not available to public bodies processing personal data in the performance of their tasks.

UK law in relation to public bodies differs from that in most other EU Member States, Cullen said. Other countries have the concept of public bodies acting outside their public tasks, something which would usually be considered *ultra vires* in Britain and therefore unlawful.

Public authorities were never intended to use legitimate interests as a processing justification and the understanding has always been that such entities should justify their processing under the "public functions" condition, said Cullen. Using legitimate interest under the GDPR would breach that regulation but for the fact that the UK has a carve-out for FOI requests, she said.

The FOI "get out" provision appears to be in Article 85 of the Regulation, which addresses specific processing situations, Cullen said. It requires member states by law to "reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression." Cullen predicted that the UK will use Art. 6 (1)(f) (legitimate interests) for FOI disclosures the way it has always done. For FOI requests, she said, the GDPR will be "business as usual."

Many questions, few answers

For public authorities carrying out non-FOI activities, the picture appears unclear.

Local authorities do have some wide-ranging powers, but when they act, they do so for the purposes of their functions and technically should not be using the legitimate interest exception, said Chris Pounder, Director at Amberhawk Training Limited. Public bodies should identify where they use the balance of interest approach, he said.

But 11KBW Barrister, Robin Hopkins, whose practice includes public and local government law as well as data protection, said it is likely that the Regulation "does not envisage scrapping the legitimate interests basis for essentially private activities of public authorities. The rationale appears to be that public functions and interests are set out in statute, so no additional interests need to be catered for. But where that does not apply, i.e. where the public authority is lawfully pursuing activities that are not fully governed by statute, it seems to me to be likely that they could still rely on the legitimate interests basis for processing."

Nothing is certain as yet, but that is at least one view," Hopkins said.

The legitimate interests prohibition should not be a problem for other activities of public bodies, Jay said. Public authorities do carry out many activities on the borders of their powers, such as fundraising, and often rely on the legitimate interest exception, but they also worry when they don't have an explicit statutory obligation, she noted.

There is a question as to what extent public authorities can rely on other processing conditions in the absence of the legitimate interests processing condition, said Linklaters data protection and technology lawyer Peter Church. Art. 6 (1)(e) permits processing "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." But "this is pretty broad," and leads to the question of how it ties into general English law public law concepts, he said. For example, if a public authority acts beyond the scope of its official authority, are those actions *ultra vires* in any event? Does that depend on the English law concept of official authority matching with European concepts in the GDPR?

Art. 6 (1)(c) permits processing for compliance with a legal obligation, Church said. The government could pass "a whole raft of new laws to provide a processing condition for public authorities," but do such bodies need a new law every time they want to do something new?

The second question arising from the legitimate interest prohibition is who is a public authority, said Church. The term as defined in recital 121 a refers to bodies subject to the PSI Directive 2003/98/EC, but might it be broader in other cases, including for example some bodies "at the fringes, such as utility companies or subsidiaries of public authorities?" Some public bodies spin off their commercial activities into a separate operating company, he said. If that operating company loses the benefit of the legitimate interests conditions, "that could be awkward."

"As with most issues on the GDPR, [there are] lots of questions but not many answers," Church said.

The Information Commissioner's Office was, at the time of writing, "waiting for the final text before making any detailed comments," a spokeswoman said. The office published a 14 March blog, and 12-step guidance checklist to help organisations prepare for the new regime[2].

One section of the guidance discusses the legal bases for processing personal data. It states in part: "Many organisations will not have thought about their legal basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your legal basis for processing their personal data..."

"You will also have to explain your legal basis for processing personal data in your privacy notice and when you answer a subject access request. The legal bases in the GDPR are broadly the same as those in the DP Act so it should be possible to look at the various types of data processing you carry out and to identify your legal basis for doing so. Again, you should document this in order to help you comply with the GDPR's 'accountability' requirements."

AUTHOR

Dugie Standeford is a *PL&B* Correspondent

REFERENCES

1 www.legislation.gov.uk/ukpga/1998/29/schedule/2
2 https://iconewsblog.wordpress.com/2016/03/14/a-data-dozen-to-prepare-for-reform, and 12-step guide at https:/dpreformdotorgdtuk.files.wordpress.com/2016/03/preparing-for-the-gdpr-12-steps.pdf

Member States' derogations undermine the GDPR

William Long and **Francesca Blythe** explain what organisations have to look out for.

The EU's General Data Protection Regulation (GDPR) was adopted by the European Parliament on 14 April 2016. The final step for formal adoption was publication of the GDPR in the Official Journal of the EU on 4 May which means that the starting date for the two-year implementation period will be 24 May 2016. Companies and data protection authorities (DPAs) will then have just 24 months from this date to implement the new requirements under the GDPR.

The GDPR is intended to create a single harmonised data protection law across the EU. However, in the text adopted by the Parliament, there are approximately 30 instances where Member States have been given the ability to legislate at a national level. This will result in national law differences in Member States and mean that businesses – even after the GDPR becomes law in 2018 – will still need to consider data protection laws in different parts of the European Union. While some DPAs will probably take a strict approach, the UK's Information Commissioner is likely to be more commercial in its approach and implement derogations which will likely assist businesses in their compliance with the GDPR. Summarised below are some of the key provisions in the GDPR which contain national law derogations.

Legal grounds for processing

In order to process personal data lawfully the processing must be based on one or more of the conditions set out in Article 6(1) of the GDPR. The conditions specified are largely the same as those in the current EU Data Protection Directive 95/46/EC (Directive) and include, for example, where the processing is based on the legitimate interests of the controller. However, Article 6(2) of the GDPR permits Member States to introduce additional requirements or specifications to ensure fair and lawful processing in relation to:

1. where the processing is necessary for compliance with a legal obligation (Article 6(1)(c)); or
2. where the processing is necessary for the performance of a task carried out in the public interest (Article 6(1)(e)).

As under the Directive, an additional legal condition such as, explicit consent, must be satisfied when processing sensitive personal data, such as data on health, trade union membership and ethnicity. However, Article 9(2)(a) of the GDPR states that even if a data subject explicitly consents, Member State law may still prohibit the processing of sensitive personal data despite consent. In addition, pursuant to Article 9(4) in relation to the processing of genetic data, biometric data or health data, Member States may introduce further conditions, including limitations, on how such data can be processed.

The GDPR also limits the way in which personal data relating to criminal convictions and offences are processed. Such personal data may be processed only under the control of an official authority (e.g. the police), or where authorised under Member State law. In both instances, appropriate safeguards to protect the rights and freedoms of data subjects must be in place.

These provisions mean that companies processing sensitive personal data, for example, those in financial services and healthcare sectors, will need to continue to check the position in each relevant Member State.

Children's data

The GDPR further introduces specific requirements for the processing of the personal data of a child. The GDPR requires that such processing in relation to the offering of information society services (e.g. through a website or social media platform) directly to children under 16 years old, or 13 years if permitted under EU Member State national law, requires the consent from the child's parent or legal guardian. This derogation, allowing different age requirements across EU Member States, could pose considerable challenges for businesses which offer ecommerce or social media services, as the age at which a person is considered a child is unlikely to be consistent. We understand, for example, that the UK has indicated it will be lowering the age limit to 13 years.

Fines and sanctions

The powers afforded to DPAs are significant including powers to suspend data transfers to recipients in non-EU countries and impose temporary or permanent bans on the processing of personal data. Pursuant to Article 58(6), Member States are also able to create laws that grant additional "corrective" powers to their DPAs over and above those explicitly granted to DPAs under the GDPR.

DPAs also have the power to impose fines for non-compliance of up to the greater of 4% of annual worldwide turnover or €20 million. Article 84(2) permits Member States to impose their own rules on the penalties applicable to infringements of the GDPR. These derogations will certainly lead to variations in enforcement powers for different DPAs and inconsistent application of fines in different Member States as currently exists under the Directive.

Accountability

Core to the GDPR are the enhanced accountability principles which require businesses to adopt and implement policies and procedures to demonstrate compliance with the data protection requirements. This in part demonstrates the shift away from the more bureaucratic approach to compliance adopted under the Directive. For example, the removal of the requirement to notify DPAs of processing

activities other than in limited circumstances (e.g. where required by Member State law in relation to processing by a controller for the performance of a task carried out in the public interest).

A key way to demonstrate accountability is the requirement for controllers to carry out data protection impact assessments where new technologies are being used or where processing may pose high risks to individuals. In addition, pursuant to Article 35(1) processors may be required to carry out such assessments prior to conducting their processing activities, if required to do so by Member State law, even where a data protection impact assessment has already been undertaken by a controller.

Controllers and processors are also required to appoint a data protection officer (DPO) if they are engaged in:

1. the regular or systematic monitoring of data subjects on a large scale;
2. the processing of sensitive personal data on a large scale; or
3. the processing is carried out by a public authority. In addition, importantly a DPO may also be required pursuant to Article 37(4) if mandated under national Member State law.

So again in relation to the core concept of accountability the principle of a harmonised EU data protection law under the GDPR appears somewhat undermined by national law derogations.

Processors

Under the GDPR, processors will, for the first time, have specific statutory obligations that they must comply with when processing personal data. These include a requirement only to process personal data on the instructions of the controller, unless required under Member State law, in which case the processor must inform the controller of these legal requirements in advance. A further derogation specific to processors provides that where the controller requests the deletion of data at the end of the provision of services, this is subject to where the processor is required to store the data pursuant to Member State law.

So companies that act as data processors, such as cloud providers, will also need to continue to be aware of national law requirements in different EU Member States.

Data Subject rights

The GDPR introduces a number of new rights for data subjects which are subject to a blanket derogation in Article 23(1) which permits Member State law to restrict the scope of these rights where such a restriction is "necessary and proportionate in a democratic society". Such a broad general derogation and further specific derogations for specific rights as described below, will lead to uncertainty as to how these rights will be applied across the EU.

One of the more talked about new rights is the statutory right for data subjects to have their personal data erased without undue delay where, for example, the consent for the processing is withdrawn and there is no other legal basis for the processing, or, in order to comply with a legal obligation in a Member State law to which the controller is subject. However, the right to erasure will not apply where the processing is necessary to comply with a legal obligation in that Member State.

Article 14 sets out the information to be provided to data subjects where the personal data have been obtained other than from the data subject. These information requirements are much more extensive than under the Directive and should be provided within one month of the receipt of the data, at the time of communication with the data subject or when the data is first disclosed to a third party. However, this information does not need to be provided where, for example, it is a Member State legal requirement to obtain or disclose such data or the data must remain confidential pursuant to an obligation of secrecy regulated by Member State law.

The GDPR also introduces new restrictions in respect of profiling, with data subjects having a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects him or her. This right is subject to a limited number of exemptions including, for example, where the processing is authorised by EU or national Member State law to which the controller is subject (Article 22 (2)(b)).

International data transfers

The GDPR maintains the current restrictions under the Directive on transfers of personal data from the EU to a third country not deemed to have adequate levels of protection by the Commission. However, pursuant to Article 49(5), in the absence of an adequacy decision, Member State law may, for important reasons of public interest, set limits to the transfer of specific categories of personal data to a third country or international organisation, providing the Member State notifies such provisions to the Commission. Once again, such national law limits and derogations on international transfers will require international companies to continue to check the national law position in different Member States.

Further derogations

Chapter IX of the GDPR sets out requirements for specific processing situations including, for example, in relation to employee data (which will impact nearly all companies) and processing for scientific research purposes (which will impact companies in the life sciences industry). In each of these situations as described further below, the GDPR provides that Member States can provide specific exemptions, derogations, conditions or rules for the processing of these types of data, giving Member States more control over the way in which such data is processed and further undermining the principle of a single, harmonised EU data protection law.

Article 88 sets out the provisions in relation to processing in the employment context. Member States can implement (either by law or by collective agreements) specific rules in respect of the processing of employees' personal data for all key purposes from recruitment through to termination of the employment relationship. Member States must notify the Commission of any such specific laws established pursuant to Article 88 without delay and at least by 2020. Any subsequent amendment affecting such laws must also be notified. The derogations in this Article 88 mean that employers of multi-national companies will likely need to comply

with a myriad of inconsistent employment laws impacting the use of employee data across Europe.

Article 89(2) provides that where personal data are processed for statistical, scientific or historical research purposes, Member States may provide derogations from certain data subject rights (including, the rights to access, rectification, restriction and objection) where such rights are "likely to render impossible or seriously impair the achievement of the specific purposes" and the derogation is necessary to meet those requirements. For companies in the life sciences industry this Article may cause concern where, for example a company is running a clinical trial across multiple Member States and the position as to compliance with these data subject rights may vary.

Additional broad derogations are set out in Article 23(1) which permits Member States to implement legislative restrictions in respect of the data protection principles and the data subject rights provided that any such restriction "respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society..." The measure must safeguard one of a limited number of factors including, for example:

4. national security;
5. the prevention, investigation or detection of crime; or
6. the protection of the data subject or the rights and freedoms of others.

Conclusion

In conclusion, the numerous derogations that exist in the GDPR undermine the core principle of the GDPR – to create a single EU-wide law on data protection to increase legal certainty for all stakeholders. The GDPR was also intended to reduce the cost of the administrative burden resulting from legal fragmentation. However, the large number of derogations and their potential broad scope is likely to result in many international companies having to continue to deal with national data protection law variations across numerous Member States to ensure compliance with the varying EU data protection requirements.

AUTHORS

William Long is a Partner and Francesca Blythe an Associate at Sidley Austin LLP.
Emails: wlong@sidley.com
fblythe@sidley.com

Government active in fighting cyber crime

Government digital services are more secure than ever, the government says. "We are building in security-by-design and taking robust action against attempts at online fraud."

The government says that the UK will substantially increase its investment to £1.9 billion to fight cyber crime. To support organisations which may have been the victim of a cyber attack, GCHQ and CPNI (UK's Centre for the Protection of National Infrastructure) have established Cyber Incident Response schemes which enable organisations to gain access to incident response services tailored to their specific needs. 31 incidents have already been tackled under the schemes, the government says.

88% of companies now actively consider cyber security as a business risk. "But businesses could do more to deepen their understanding of the threat: less than a third (30%) of boards received high level cyber security intelligence from their Chief Information Officer or Head of Security, while less than a quarter (24%) of companies based their cyber risk discussion on comprehensive or robust management information," the government says in its annual report on cyber security.

• *See the annual report on cyber security strategy www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report.*

Blacklisted workers win compensation from big construction firms

Around 700 workers who were blacklisted in the construction industry have secured damages ranging from £25,000 to £200,000 per claimant in out of court settlements, the *Guardian* reports. The total payout could be as high as £75m. Allegedly a number of companies have also apologised to the workers for the anxiety and stress they caused.

The blacklisting was revealed by a whistle-blower in 2006.

The construction firms had been checking employees against the blacklist before they were hired. The personal data collected included details of trade union membership and activities and employment history. The information was often incorrect and employers were denied employment without any reason.

The blacklist was kept by the Consulting Association, which was subject to an ICO investigation, and fined £5,000 for a data protection offence.

• *For background information, see PL&B enews from 2009 www.privacylaws.com/Publications/enews/UK-E-news/Dates/2009/8/PLB-UK-E-news-Issue-93/*
See www.theguardian.com/business/2016/apr/29/blacklisted-workers-secure-compensation-construction-firms

Royal Mail becomes certified online identity provider

The user-centric programme benefits from having privacy built in from the start. **Laura Linkomies** finds out how Royal Mail prepared for its role as an identity provider.

The government has now appointed eight certified external identity providers, including Royal Mail, who make it easier and more convenient for individuals to access public services. It takes only 10 minutes to verify identity online using GOV.UK Verify. An individual's identity is verified by a certified company each time he or she wants to access a service. Individuals may choose one certified company, or use several. The system, which is free of charge, does not create a centralised database, but is based on data matching and user-centric identity management.

Stephen McCartney, Director of Information Governance and DPO at the Royal Mail Group told *PL&B* that the system strictly limits the amount of information that is collected, and its use. Royal Mail is not allowed to use the data for its own purposes – so what was the motivation to join the scheme?

"It is part of Royal Mail's continuing development on how we have protected individuals' privacy and confidentiality for the last 500 years. The mail service was set up to be a secure communications channel and again today we have a responsibility to protect privacy, security and integrity of the universal service we provide. However, we are witnessing a move to a more digitally enabled environment and Royal Mail also provides services in that environment. So it is a natural evolution," McCartney said.

Jim Conning, Managing Director of Royal Mail Data Services added: "This enables much easier interaction between the citizen and government. Royal Mail currently delivers to 29 million UK addresses and thus has expertise in how to deal with complex data, and manage a secure redirection service. Citizens can now interact with the government in the way that is convenient for them. Trust is the key."

Royal Mail is the lead in consortia where Royal Mail is the Identity Provider and uses two technology partners to provide different parts of the process – the GB Group for the verification process and Avoco for access. It received the certification as identity provider mid-March, and the take-up has been good. So far, half a million user identities have been verified through GOV.UK Verify[1].

There are currently seven other certified companies; Barclays, CitizenSafe, Digidentity, Experian, Post Office, SecureIdentity and Verizon. Before they could join GOV.UK Verify, they needed to go through formal processes with the Cabinet Office. The government required the companies to meet industry standards for information security, and to be certified by an independent body (such as tScheme) to confirm that they meet government standards for identity assurance, are compliant with the requirements in their contracts with the Cabinet Office, and are compliant with data protection law.

> "We are constantly measured against our performance as part of the tScheme certification."

The nine services currently available for access on GOV.UK Verify platform range from getting a pension statement or filing a tax return to viewing your driver's licence information. It is expected that another 15 services – such as a possibility to view health records or sign mortgage deeds – will be added in the next 18 months.

Certification process

tScheme is an independent, non-profit making, industry-led body set up to approve identity services. tScheme requires all certified companies to meet a number of requirements – which include the security standard ISO27001. McCartney said that they cannot reveal details of the security policy or type of encryption used, but Royal Mail is meeting more than the baseline industry standard.

McCartney: "We are constantly measured against our performance as part of the tScheme certification – I am not aware of any plans for an audit just yet. But it was an absolute requirement to conduct a Privacy Impact Assessment (PIA) for becoming a certified provider. The PIA has not been made public because it focuses on security and our security protections. When we receive information from individuals to identify them, we only keep a certain proportion of that information. We cannot use it for any other purpose than identity assurance, and audit. So the PIA as such was therefore quite limited in scope."

The government requires certified companies to be clear and transparent about how they process personal data submitted during the identification process. The companies' privacy policies must comply with relevant legislation and regulations in their sector.

McCartney said that Royal Mail did not, however, have to make any changes to its privacy programme – the privacy statement for Royal Mail is very specific for the activities of Royal Mail as a whole. The information collected under the identity assurance scheme will never fall under Royal Mail's privacy policy because it is used purely for the purposes of processing the ID validation.

Identity checking process

When an individual seeks to have their identity verified online, the platform

will request users to first provide basic personal details. Each provider has a slightly different set of requirements. In order to use Royal Mail Identity Verification an individual will need: A UK driving licence or UK passport (ideally both), and bank account or credit card details (ideally both). After these basic questions, the programme asks individual additional security questions about statements, online accounts, mortgage payments, or utilities/mobile phone contracts.

McCartney: "You will perhaps be asked questions about your current credit or similar that verifies your identity. There is no credit reference check involved and the process does not affect the credit score."

The data is matched with authorities such as the DVLA but with the full knowledge of the individual. If the information given matches successfully with the agencies in question, users will be given a unique online identity.

McCartney: "The data that we use for data matching is retained for a maximum of 180 days as required by auditing standards. We retain the information of the applicant's actual identity for as long as 30 days if data is not successfully matched, and we then delete it."

Conning explained that the government does not know which identity provider is verifying the identity of an individual, and Royal Mail does not know which government department has access to the information – the citizen is in charge. There is full transparency and individual control. Individuals can use any identity provider, or indeed the existing government gateway.

The government information on GOV.UK Verify says that the Identity Provider (IDP) Picker Service asks the user a few simple questions to recommend the most appropriate identity providers for their needs.

The service does not gather sufficient information to identify the user, nor is that information retained in a form that could be used to render it identifiable at a later date. The information is dropped one hour after the session, but aggregated results are used in anonymous form for user experience analysis.

Third party access and dispute resolution

If individuals have complaints during the process, they can raise the issue online at the time of the verification process.

Conning: "If someone has a general data protection complaint they would go to the ICO. Other issues to do with the verification process can be sorted in real time online. Our call centres have a process geared up to helping individuals. We are responsible in helping them through the process but ultimately their issue would be resolved by the government department in question."

McCartney: "Third-party access is allowed only in exceptional circumstances and with parliament's approval. We would need to have a basis in statutory law for any third party to access the information that we hold. I can only see that happening in circumstances where a crime is suspected and there is evidence – but these are really limited circumstances. We do not provide any access to the data we hold."

Privacy has been built in

GOV.UK Verify is a replacement for the unpopular ID card scheme. The Privacy and Consumer Advocacy Group[2], set up by the Cabinet Office in 2011 specifically to advise on identity assurance, defined the standards of the programme. Participants include representatives from No2ID and Big Brother Watch, consumer champions like Which? and leading academics from the LSE, UCL and the Oxford Internet Institute. Some of these people were previously opposed to the ID scheme, McCartney said.

"It has been a joy, as a privacy professional, to work on a project that has been designed so well in terms of privacy. For example, PIA was built into the design of the whole programme."

"I have been working in privacy for 15 years and during that time government policy has grown with the growth of the digital environment. The government departments that are now driving this user-centric model are the same that were behind the national identity scheme. The government's understanding of the digital marketplace has grown, people are digital natives and the digital market works a bit differently."

McCartney said that there have been very few privacy challenges with this programme. The past government policy on ID was very different – GOV.UK Verify benefits from user-centric identity management, which means that the user is able to control their identity and have choice between the identity providers.

"When we did the PIA it was evident that there was so little scope for the identity providers to use the data in other ways as the scheme has been designed so comprehensively around the individual. The area where we needed to do some work was the security architecture. The government stated what standard was needed and we worked towards that so it was a fairly simple process."

Future prospects: Private sector and NHS take-up?

No legislative changes were needed to run this programme but the EU General Data Protection Regulation (GDPR) will soon set a new data protection standard in the UK. However, McCartney thinks that the system has been designed so that it goes beyond compliance with the current UK Data Protection Act.

"We will not have to change very much to fit in with the GDPR. People choose the provider, and can stop processing any time – individual rights are very much at the core of the programme. Looking at the GDPR, I struggle to see how this programme would fall behind the new law."

The GDPR will introduce the concept of data portability – individuals can transfer all of their data to another provider. "In this programme, you would just provide the same data again. Individuals can easily choose another identity provider. We do not have to worry about implementing this provision as it is already there."

McCartney said that while there may not have been a conscious choice to fit in with the GDPR and future proof against it, choosing a very high standard of user-centric identity management has effectively ensured that this is the case.

As to the future of online identity verification, the government says that there are some plans to extend the programme to the private sector; it is

working with industry to consider the practicalities of private sector re-use. In the first instance, it is planned to extend the programme to the NHS. The Cabinet Office is currently working with the Liverpool Clinical Commissioning Group to understand how GOV.UK Verify could meet their needs. "We are not at the stage of reporting outcomes yet," the Cabinet Office said.

INFORMATION

www.royalmail.com/personal/identity-verification/faqs
https://gds.blog.gov.uk/2014/01/23/what-is-identity-assurance/
www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

REFERENCES

1 As of 22 April – information from the Cabinet Office. Performance data is published at www.gov.uk/performance/govuk-verify/total-authentications
2 www.gov.uk/government/uploads/system/uploads/attachment_data/file/448101/IDA_Privacy_and_Consumer_Advisory_Group_-_ToR_PDF.pdf

PRIVACY AND CONSUMER ADVOCACY GROUP CONTINUES ITS WORK

Jerry Fishenden, Chair of the Privacy and Consumer Advocacy Group provided an insight into GOV.UK Verify and an update of the group's work:

***PL&B*: There seems to have been a huge change in the government's approach to privacy in identity assurance. Why do you think that is?**
Fishenden: I think a lot was learned from the experience of trying to impose a flawed national identity card and its associated honeypot register based on simplistic ideas from the 1940s. On the back of this, there was a recognition of the need to regain and improve trust with the general public, and to apply better computer security engineering. With the increase in cyber-crime and online fraud, there has been a growing recognition of the need to better secure personal data, including the government commitment to place citizen data under citizen control. Ensuring online, trusted identities is a precursor to being able to deliver any secure, trusted services online – if not well designed, the move to digital public services will fail.
Worse, if our personal data and identity-related data is not better protected and continues to be shared around as services becoming increasingly digital, fraud will increase not decrease.

***PL&B*: Do you think the identity assurance principles address all relevant privacy issues relating to this programme?**
Fishenden: The principles relate specifically to aspects of privacy associated with the identity assurance programme, which is only a subset of overall privacy issues. The principles are also intended to evolve and improve as the programme develops rather than be chiselled in stone for all time. The nine principles "assume that an Identity Assurance Service is mature and well established", which is clearly not yet the case. The principles also explicitly acknowledge that "in the early stages of its development there may well be a phasing-in period in relation to each Principle, or that in some cases a Principle might need a degree of initial flexibility".

***PL&B*: As the scheme is up and running, what is the role of the Privacy and Consumer Advocacy Group now?**
Fishenden: The group will continue to monitor and review the operation of Verify as it develops. However, the Privacy and Consumer Advisory Group (PCAG) has a wider remit than purely identity assurance. The Minister for the Cabinet Office (MCO) tasked it with advising the government on how to provide users with a simple, trusted and secure means of accessing public services. The group's overall remit is to ensure best practice in identity, privacy, security and technology to protect citizens' interests, with a particular focus on ensuring data and personal information, and the technology used to manage it, is well designed, engineered and implemented. For example, the group will be calling in the 'Better use of data' proposals for review[1].

***PL&B*: Can you comment on the relationship between GOV.UK Verify and the Investigatory Powers Bill – is there a clash with the Bill's requirement on data retention?**
Fishenden: The IP Bill contains numerous areas of concern. The Group is currently discussing its response.

1 www.gov.uk/government/groups/privacy-and-consumer-advisory-group and https://identityassurance.blog.gov.uk/2015/09/11/gov-uk-verify-identity-assurance-principles/

High Court decides on 'abuse' of SAR process

A High Court case, *Gurieva & Anor v Community Safety Development (UK) Ltd* [2016] EWHC 643 (QB) of 6 April 2016, shows some emerging trends in subject access litigation. The judge said "I have difficulty with the notion that the use of a SAR for the purpose of obtaining early access to information that might otherwise be obtained via disclosure in pending or contemplated litigation is inherently improper."

The claimants allegedly used the Data Protection Act to gain an illegitimate procedural advantage in criminal proceedings which have been brought against the claimants. The defendant, Community Safety Development (CSD), argued that the SAR represented a misuse of the information rights conferred by the DP Act.

The judge ruled that the claimants' SAR is and was valid. "There was never any proper basis for questioning its validity. CSD's failure to disclose any personal data at all represents a breach of the claimants' rights. The personal data held by CSD that relates to the claimants may include some that is protected by the crime exemption, and some that is protected by litigation privilege, but it has not been proved that all of it is so protected. The reason for that is that CSD has not carried out the necessary analysis. I am not satisfied that enforcement would be disproportionate, or that the SAR or these proceedings represent an abuse of the claimant's rights or an abuse of process. It would be wrong for me to carry out the analysis in place of CSD. There is no good reason not to exercise my discretion in favour of enforcing the duties imposed by the Act."

• *See www.bailii.org/ew/cases/EWHC/QB/2016/643.html*

Data Protection in the new world of Artificial Intelligence

Artificial Intelligence may pose new challenges that do not fit in under the EU Data Protection Regulation. **Nicola Fulford** and **Gemma Lockyer** explore the issues.

A quick online search of "what is AI?" does not provide you with an easy answer and this is because artificial intelligence can have different meanings to different people. For our purposes, it is a computer system which is able to perform tasks which would normally require human intelligence.

To date, as lawyers, we have needed to deal with computers and machines which are capable of numerous and speedy computations and calculations – but these actions have all been governed by the direction of the programmer. Artificial intelligence, on the other hand, is the machine intelligently thinking, learning and making decisions and actions based on this thought and knowledge. From a legal perspective this phenomenon challenges many key legal concepts and means that we need to address how we apply core principles of personality and liability onto something the law is not yet ready to deal with.

Could an AI be a data subject?

A data subject is defined as any individual who is the subject of personal data. Typically we think of data subjects as employees, contractors, customers or individuals on a marketing database etc. A limited liability company is not a data subject for the purposes of the Data Protection Act 1998 (the DP Act) and neither is a computer system. An AI is capable of performing tasks which would normally require human intelligence and so could it be argued that an AI should be given some of the same protections given to humans?

The current DP Act's definitions means that there is not going to be any personal data recorded in relation to an AI data subject because personal data relates to "a living individual" who can be identified from the data. Even if we can acknowledge that an AI has human intelligence and should be classed as an "individual", and therefore a data subject, would we be able to go as far as to describe it as living? And, perhaps more importantly, should we? Given the new definition under the EU General Data Protection Regulation (GDPR) changes this to a "natural person", that does not seem to be the direction of travel.

Processing data using Artificial Intelligence

A much more real concern for businesses is the use of AI in the processing of personal data. Processing is very broadly defined and includes "obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data". The first data protection principle, which requires fair and lawful processing, is often met through the use of consent. The individual will consent to the processing of their personal data and this will enable the processing to be fair.

How can we obtain informed consent when the processing of the data is no longer a predictable response to a set of pre-defined instructions given to a computer programme by a programmer but is now the result of an autonomous machine which is learning and thinking for itself? The programmer no longer knows what the next processing operation might be because that is a decision taken by the AI. Consent is not mandatory in the UK for the processing of personal data, although it is often the easiest way to justify the processing. Without consent the data controller will (generally) need to show that the processing is necessary for a contract or is for legitimate reasons, provided these reasons are not outweighed by the privacy implications for the individuals concerned. However, given that we don't know exactly what processing the AI might undertake in relation to the data it is given, how can we know that the processing is necessary? Similarly, without understanding the processing and what the privacy implications may be, how can that balance be understood and documented?

Impact of the GDPR

The current EU data protection regime is due to be replaced by the GDPR. There are several key changes in the GDPR which will affect those working within the sphere of AI.

The first is the requirement to implement Privacy by Design and by default. Businesses will be required to take data protection requirements into account from the inception of any new technology that involves the processing of personal data. An AI works because of its ability to process large volumes of data and quickly. IBM's Watson – a computer capable of answering questions framed in natural language thanks to the vast database of information it has access to – is an example of this. If the AI is given access to personal data as part of that database, then the AI will be processing personal data and data protection requirements will need to be taken into account as part of its design. This may not always be possible when the machine itself is evolving as it thinks and learns for itself.

Thanks to the increased computing power of AI it may be possible that data which might previously not have been considered personal data, because from the data alone you could not identify a living individual, might become personal data because the AI has access to other information which, when processed together with that data, could be used to identify a living individual. This potentially increases the scope of personal data which might be available relating to a data subject.

The GDPR also restricts profiling which is the automated processing of personal data and the use of personal data to evaluate certain personal aspects relating to a natural person, for

example analysing or predicting aspects concerning a natural person's economic situation or personal preferences. Pursuant to Article 14(1) of the GDPR, data subjects have a right not necessarily to avoid profiling itself, but rather to avoid being "subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Recital 58 provides as examples the "automatic refusal of an on-line credit application or e-recruiting practices without any human intervention". Consent to this profiling will need to be obtained and this will need to be considered well in advance of implementing these kinds of AI.

Are we ready?

Artificial Intelligence is a reality and with "big data" becoming "bigger data" all the time, is the legal data protection landscape ready for AI machines? The emphasis, we believe is going to be on ensuring the data controllers are able to build in parameters around privacy into the AI, and also in trying to obtain the necessary consents before transferring data to an AI. Consent can be tricky today, but with the GDPR, consent will become even harder to obtain.

As with other new technologies, the law inevitably plays catch-up and AI will surely throw up new situations that do not "fit" what was in contemplation for the GDPR. For example, whether the AI is capable of being a data controller itself, making its own decisions in relation to the processing of the data, or how we might impose any liability on the AI for anything it did in breach of the DP Act or the GDPR. Given the power of the technology, this is a field likely to see an emphasis on ethics as well as law.

AUTHORS

Nicola Fulford is Data Protection Partner and Gemma Lockyer is Commercial Technology Associate at Kemp Little LLP.
Emails: Nicola.fulford@kemplittle.com
Gemma.lockyer@kemplittle.com

Degradation of privacy standards could be deemed abuse under competition law

The UK Parliament's European Union Committee, in its report issued on 20 April – titled "Online Platforms and the Digital Single Market, (HL Paper 129 – says that online platforms are a prime example of tension between DP and competition law. The House of Lords committee stresses that dominant online platforms could potentially abuse their market position by degrading privacy standards and increasing the volume of data collected from their users. If one provider has multiple sources of user data, it may prove to have an unmatchable advantage over individual online platforms, making it difficult for rival platforms to compete.

The committee criticises large online companies for not fully explaining to consumers how their personal data may be used. As a result, trust in how online platforms collect and use consumers' data is worryingly low and there is little incentive for online platforms to compete on privacy standards, the Lords say. "We believe this presents a barrier to future growth of the digital economy. Online platforms must be more effective in explaining the terms of such agreements to consumers."

Online platforms must accept that the new EU Data Protection Regulation will apply to them and will be enforced, and prepare to make the necessary adaptations, the committee says. The new data portability provision will be a significant change. It could promote quality-based competition and innovation by making it easier for consumers to switch platforms.

The EU Committee is concerned that the principle of data portability in the GDPR may unravel in practice. "If applied too rigidly, it could place onerous obligations on emerging businesses; however, unless it is more clearly defined, it is unlikely that it will be implemented by many online platforms."

The EU Committee urges the EU Commission to publish guidelines explaining how data portability requirements apply to different types of online platforms. The EU Commission, the UK government, regulators and industry should use the following two years - the time before the Regulation enters fully into force - to ensure that its terms are well understood and effectively implemented.

In addition to the GDPR, the EU e-Privacy Directive will be relevant. The European Data Protection Supervisor, Giovanni Buttarelli said on 9 November 2015, when providing evidence to the Select Committee on the European Union's Internal Market Sub-Committee, that the existing e-Privacy Directive focused "more on standard telecom providers and electronic communication services", and was hard to apply to platforms. The ICO said the extent to which the e-Privacy and Data Protection Directive applied to online platforms had "been a contentious issue for many years and some online platform providers have argued that they are only processing 'pseudonymous personal data'—and should be subject to light touch regulation." However, the ICO considered "that search engines are data controllers and are processing personal data when, for example, they deliver name-based search results." The ICO agreed that "passively-collected information can identify data subjects".

• *European Data Protection Supervisor, Giovanni Buttarelli, will speak about "How data protection rules should be enforced in tandem with competition and consumer policy" at Great Expectations, the Privacy Laws & Business 29th Annual International Conference, 4-6 July 2016. See www.privacylaws.com/annualconference.*

See the Lords report at www.publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/12902.htm

How Transport for London protects customer privacy

With around 4 billion journeys per year, 26 million Oyster cards in use, and 21,000 CCTV cameras, Transport for London (TfL) has to sustain public trust during 31 million daily journeys. **Stewart Dresner** finds out how TfL's privacy and transparency processes work.

TfL is in charge of London's buses, Underground trains, Overground trains, the Docklands Light Railway, Tramlink, River piers, main roads, traffic signals and the cable car across the River Thames. James Newman, TfL's Privacy and Data Protection Manager told *PL&B* in an interview that the scope of personal data processed by the organisation is immense. It includes:

1. 26 million Oyster cards used per year of which 4 million are "registered" cards
2. 8 million contacts in TfL's customer database, including 4.5 million e-mail addresses – 300 million service information emails were sent in 2015
3. 1.7 million active Congestion Charge/Low Emission Zone customer records
4. 200,000 registered Santander Cycles customers
5. 100,000 licensed taxi/private hire drivers
6. 47,000 registered Dial-a-Ride users
7. Images from 21,000 CCTV cameras
8. Data from 1,400 Automated Number Plate Recognition (ANPR) cameras directed at vehicles
9. Mobile device WiFi and Bluetooth connection data
10. Penalty Fares and associated prosecutions for failing to pay for travel
11. Penalty Charge Notices and associated prosecutions for vehicles committing traffic contraventions.

Therefore, TfL has access to vast information resources both in real time and for planning purposes. Protecting personal information is essential to assure the individuals whose data is processed that it is being held securely and used only for the purposes for which it was collected and properly related purposes.

TfL's website as the primary communication medium

James Newman explained that processing standard subject access requests is managed by providing on TfL's website clearly written and designed subject access forms to help requesters submit the information needed to speed the response process.

In a model of layered privacy notices, there is a substantial section of the TfL website on Privacy & Cookies[1] which currently has 16 sub-sections, for example, on access your data, CCTV, contactless payment, Oyster Card, and Santander Cycles, the bicycle hire scheme. Each of them opens to reveal several sub-sections, all written in plain language and in short sections so anyone can find their way to the information they want – see the Santander Cycles box (p.19).

When there have been updates, there is a statement, such as "A number of updates to the policy were approved by the Commissioner and TfL Executive Committee on 17 March 2016" but there is no indication what has changed.[2] However, Newman explained to *PL&B* examples of these changes:

- 'Privacy Impact Assessments' must be carried out as part of the development of any new business process or IT system, which will be used to process personal information
- all employees directly involved in processing personal information are to complete privacy awareness training every year
- responsibilities of 'Personal Information Custodians' (a group of around 60 Heads of Department or Directors responsible for business/operational activities involving the processing of personal data) need to be stated
- serious or repeated breaches of the policy may be treated as misconduct in accordance with the TfL Code of Conduct and relevant HR policies
- TfL will be open and transparent about how personal information is used, requiring customers to opt-in to receive marketing communications
- any actual or suspected incident involving the loss, theft, unauthorised disclosure, accidental destruction, or other compromise of personal information should be reported to [the] Cyber Security and Incident Response Team.

Newman explained "Customers place a huge amount of trust in TfL when they provide us with their personal information, so it's really important for all of us to treat it with respect and comply with our own policy as well as privacy and data protection legislation."

Priority areas

Newman has selected several priority areas. While the EU General Data Protection Regulation and the companion EU Directive on police and criminal justice now demand attention, TfL has already adopted some of their provisions.

For example, there was a two month exercise conducting a Privacy Impact Assessment (PIA) on body worn CCTV which is used by Revenue Control Inspectors (ticket inspection) staff and others who might be vulnerable to hostile action from the travelling public. Images collected have evidential value in the event of a legal dispute. The website statement shows the results of this PIA:

"Some TfL employees are issued with body worn cameras, for example, Revenue Control Inspectors on the London Underground network. These devices are able to capture audio recordings as well as images. The cameras are clearly visible and only switched on in the event of an incident (for example the member of staff being subjected to verbal abuse or threats of violence)." [3]

TfL has several contracts with external organisations to manage parts of

SHARING SANTANDER CYCLES DATA

Example of a TfL Privacy Notice:
We share information only in very limited circumstances. We share users' personal data with our subsidiaries and service providers for the purposes of customer services and administration, to provide travel-related information and for customer research and fraud prevention.
In the event that you make a claim on the scheme's Public Liability Insurance for yourself or on behalf of an additional user we will, on request, share relevant information with the insurance provider or their agent for the purposes of verifying and processing your claim.
TfL will share your personal information with the scheme's sponsor for marketing purposes where you have explicitly agreed that we can do so. You can opt out from receiving marketing information from the Scheme Sponsor at any time by amending your marketing preferences via your online account or by telephone on 0845 026 3630.
We may also disclose personal data if required to do so by law. The Data Protection Act allows us to do this where the request is supported by evidence of the relevant legislation which requires the disclosure, or a court order.

https://tfl.gov.uk/corporate/privacy-and-cookies/santander-cycles

their personal data responsibilities, for example, with:

- Experian to handle the consequences of data breaches, including the provision of ID theft protection and credit monitoring services to affected customers
- Capita to process road user charging data
- Cubic Transportation Systems to process electronic ticketing data
- SAP to process TfL's human resources data, partly via a cloud-based service to map the skills available against work force planning for future needs.

In every case, TfL will ensure they know exactly where the personal data is to be processed and include comprehensive privacy and data protection contract terms.

TfL is often approached by organisations to buy its personal data but so far it has refused. The sponsorship arrangement with Santander for London's bike hire scheme means that Santander does have access to user contact details, but this only extends to customers who explicitly opt-in to this use of their data for marketing purposes and they can opt out at any time (see box). An app is available – developed by Serco, the outsourced service provider which manages the bike hire scheme – that shows users where to find available hire bikes and makes payment easy.[4]

Use of contactless payment cards is rapidly increasing. TfL is the fastest growing contactless merchant in Europe. One in seven contactless transactions in the UK takes place on TfL's network which is managed and protected in accordance with the PCI DSS data security protocol.

TfL draws together a vast array of data sources into its Big Data programme. It tracks social media, in particular, Facebook and Twitter and explains its monitoring policies.[5] These policies deal with both operational issues and analysis of trending sentiment by social media users on their experience of TfL services. Such service feedback could cover anything, such as poor standards on stations, late trains, accidents, faulty traffic lights, or good customer service by TfL staff.

When things go wrong

The Information Commissioner's 2014/2015 Annual Report said that "An employee of Transport for London was prosecuted [by the Information Commissioner] for unlawfully accessing Oyster card records of family members and neighbours."[6] Newman explained that this case, heard at the Westminster Court in early 2015, involved a TfL employee who stalked an individual by illegally accessing their Oyster Card use and tracking their journeys. Following the termination of their employment with TfL, the individual was convicted and fined £1,000 plus costs, by the court. TfL worked closely with the ICO prosecutions team to ensure that the appropriate evidence, including detailed system access logs, was made available to the court.

Open data

TfL has a policy to encourage software developers to use transport data feeds "to present customer travel information in innovative ways." However, the compulsory terms and conditions include the requirement that "This Licence does not……include personal data in the Information" [provided to users]. Another condition is "TfL's Privacy Policy will apply to all personal information collected in connection with Your use of the Service"[7]

Transparency and FOI

TfL has a detailed Transparency Strategy and is subject to the Freedom of Information Act.[8] Changes in recent years include publishing much more information, such as lowering the amount covered by its policy on releasing information on contracts and tenders with a value of over £5,000. All expenditure of more than £250 is now published. Information is available every quarter on internal audits carried out, for example, on data centres which included a line on "response to access requests."

TfL publishes information proactively on the subjects on which it receives frequent FoI requests.[9] TfL receives around 2,500 Freedom of Information (FOI) and Environmental Information Regulations (EIR) requests every year. TfL currently provides a full response to 85% of them within the statutory time limit, for which there is a standard time limit of 20 days.[10]

REFERENCES

1 See www.tfl.gov.uk/privacy
2 https://tfl.gov.uk/corporate/privacy-and-cookies/privacy-and-data-protection-policy
3 https://tfl.gov.uk/corporate/privacy-and-cookies/cctv
4 https://itunes.apple.com/gb/app/santander-cycles/id974792287?mt=8
5 https://tfl.gov.uk/corporate/terms-and-conditions/social-media
6 https://ico.org.uk/about-the-ico/our-information/annual-reports/ See 2014/15 Annual Report, p.25
7 https://tfl.gov.uk/corporate/terms-and-conditions/transport-data-service
8 https://tfl.gov.uk/corporate/transparency/
9 https://tfl.gov.uk/corporate/transparency/#finance-operations-performance
10 https://tfl.gov.uk/corporate/transparency/foi-performance

It is time to get GDPR compliant

The EU General Data Protection Regulation is now here to stay and will form the new DP regime in the UK from 25 May 2018 onwards. **Laura Linkomies** reports.

The EU General Data Protection Regulation's (GDPR) accountability requirements mean that organisations have to demonstrate the steps which they have taken to comply with the provisions – effectively this means having a trail to show the measures which they have taken. For multinational companies, many of these steps may already be in place but the Regulation also brings completely new aspects such as the Right to be Forgotten and data portability. All organisations will need the next two years to get their house in order, and should start work now.

Speaking at a conference in April in London, Nicola McKilligan-Regan from Privacy Partnership said that organisations should start seeking approval for their project budget now, if they have not already done so.

She said that a key mistake is to fail to plan properly and kick off a project prematurely – "there is no point running in the wrong direction," she said. "Things may change during implementation as requirements become clearer but these must be covered by a change management process not just added in."

Translating the GDPR into practical actions

Organisations could start by identifying which aspects of the GDPR will have most impact on their business. A risk assessment and gap analysis can be a start to identifying how to use sometimes scarce resources.

Bridget Treacy, Partner at Hunton & Williams, speaking at the same event, said that in the UK, a DPO has traditionally worn many hats and now this person will suddenly be responsible for everything. DPOs need to have a team and it might make sense to have the statutory DPO and in addition another person who is more of a privacy strategist.

Nina Barakzai, Group Head Data Protection & Privacy, Sky UK Limited said that her company already has this model. She reports to the audit committee, and data protection is treated as a board-level issue.

"People come to me with their ideas and suggestions on how to include privacy in business. It is quicker for them to have new products approved this way. Privacy is already on people's radar. Each business area is empowered to be responsible for privacy work and implement data protection."

She said that in their preparation for the GDPR, they went through all the articles and identified some 45 issues that needed to be dealt with. They then identified the most important ones in any business area depending on which issues were critical or involved the most personal data.

She said that the five-year business plan includes an assessment of risk and a timetable for issues that take the most time and money.

"We focus on assurance, not compliance. Business moves forward fast – sometimes the Regulation is already behind business developments."

Helen Gourdin, Senior Counsel, Global Compliance at Diageo plc said that her company has a steering committee to work on these issues. GDPR can be divided into specific areas. Documentation is required on any action taken. A good starting point is to look at the Article 29 Working Party work programme to see which issues they prioritise.

She said there was still a lot of uncertainty – especially on the employee side. "We have been making step changes for example to our privacy policy. The ICO's 12 points on GDPR are useful but we have also put in specific requests for further guidance on issues such as breach management. What kind of filing will be needed? What about cyber breach notification?"

William Malcolm, Senior Privacy Counsel at Google, said that in most cases Google already has a mature privacy programme but now it needs to demonstrate accountability to Data Protection Authorities and users, also to users. The GDPR is only one facet in the Google privacy programme, he said. He thought that many issues in the GDPR are very clear and they can start the work now.

"Harmonisation is the key. The DPAs are to define high risk processing – there is a responsibility on the European Data Protection Board (EDPB) to issue guidance. Organisations and DPAs must start a dialogue on this and also on the scope of delegated acts. We want a world-class privacy programme but need clarity in regulatory expectation."

Treacy observed that there are competing regulatory frameworks. Also the GDPR includes some 40 exemptions that provide a 'margin of manoeuvre' for Member States, the EU Commission or the EDPB.

It has to be noted that the EDPB is empowered to take legal action and challenge DPA decisions. The recitals in the GDPR explicitly say that there is this "margin of manoeuvre for Member States to specify its rules" (for the processing of personal data).

Barakzai noted that they are concentrating on the clear areas. But there is no point in stopping and waiting for guidance as certain things need to be done.

"We have created a set of guiding principles that will work in the GDPR context. We are mainly looking at concepts, not the individual GDPR articles."

> "Google: We want world-class privacy programme but need clarity in regulatory expectation."

Individual rights

Google has done much work in this area. It is important to be transparent and build practical tools, Malcolm said. He said Google can use its existing tools and design controls for data portability. Individuals can control their data and search histories.

"We are committed to Privacy by Design. We have invested in a privacy engineering team for many years now but there is more work to do."

Gourdin said that they are working on Diageo's digital transformation programme – a very ambitious programme to ensure transparency and control. "We work hard to fit privacy into our strategy."

Public-sector issues

"Better use of information is central to delivering our services more efficiently," Amanda Hillman, Team Leader, Data Sharing and Data Protection Policy Team at the Department of Work and Pensions (DWP) said at the Westminster eForum. "Privacy by Design is essential to gain customer confidence."

Most government offices do not have a DPO, she said, but a Senior Information Risk Officer, or similar. "Now we have to change the culture so that the person doing the job will have reassurances that we are doing the right thing. We have to address individual rights."

She said that the DWP receives more Subject Access Requests (SARs) than all other government departments put together. The data they hold is incredibly sensitive. The GDPR will require a quicker turnaround in responding to SARs – a month instead of the 40-day period that currently applies in the UK.

"Our governance structure will have to be revamped: how we do things and when. A carrot and stick approach to enforcement will work – telling senior officers of the culture change needed but also of the large fines. In this respect the GDPR helps me."

She said that for the DWP, some of the most important compliance issues are profiling – what does that mean – and automated processing – what does that mean under the new definitions? Additional aspects that need careful consideration are data portability and how to provide a fair processing notice that can be understood by everyone, but at the same time satisfy the legal requirements. She said that they are using the layered approach.

She said that there was no decision yet on whether there would be a single government model for compliance – they are waiting for news from the Department of Culture, Media and Sport.

Cooperation needed

Fedelma Good, Director, Information Policy & Business Controls, Personal & Corporate Banking, Barclays, said that consumer trust will equate with commercial benefit.

"Commercial opportunities will come to those who are working on GDPR implementation now." Barclays worked together with different sectors at the time of the e-privacy Directive's drafting and the troublesome question of cookie compliance. "We decided to aim for a consistent version of cookie compliance."

We now need to achieve consistency in how privacy policies are presented to the individual, she said. "There is a huge opportunity in the digital space. One of the best examples of layering is the DMA [Direct Marketing Association] code of practice."

Chris Combemale, Executive Director at the DMA, said that now is the time to embed the right privacy culture in organisations. Consumer attitudes to privacy are increasingly critical, he said. In a DMA survey, 58% of those interviewed said that trust is the most important issue when they decide whether to share their personal data with businesses. People would like more control over their data – 81% believe that data is theirs to exchange for value. Only 7% believed that they obtained the most benefit from the data exchange with a company. The DMA has a specific GDPR section on its website. The main issue is to put the customer first.

Simon Rogers, UK Privacy Lead at IBM, said that they need to act now to structure the company response to GDPR.

"You need to focus on the gains, not just the compliance. So how can we better leverage technology? Do not just talk about the fines but think about this in a wider holistic scope."

"Global large organisations need someone who takes responsibility and acts as a lead in GDPR preparations. I suggest starting this as a project and pulling in other parts of the business. It is not just about privacy but a larger question of information governance and security."

"Make sure you break the law into bite-sized chunks, conduct a gap analysis and a Privacy Impact Assessment," he said.

EU DP Regulation will apply on 25 May 2018

The EU Data Protection Regulation was published in the European Union's Official Journal on 4 May. It will start to enter into force on 24 May this year, and will apply from 25 May 2018.

Together with EU Regulation 2016/679, the European Commission has published the text of the so-called Police Directive and the Passenger Name Record Directive.

By 25 May 2020 and every four years thereafter, the Commission will submit a report on the evaluation and review of Regulation 2016/679 to the European Parliament and to the Council. These reports will be made public.

Businesses now have two years to start their preparation process. Join the main players with 40+ speakers from 16 countries at Great Expectations, *PL&B's* 29th Annual International Conference, 4-6 July at St. John's College, Cambridge to learn how to work towards your organisation's compliance.

The full conference programme has now been published at www.privacylaws.com/ac29

• *The text of the Regulation – in all languages – is available at http://bit.ly/1T5Y5s3*
The 'Police Directive' is at http://bit.ly/1T5Y5s3 and the 'Passenger Name Directive' at http://bit.ly/1VONjqB

ICO issues Undertaking on HSCIC

The ICO has issued an Undertaking – a written commitment to take action – on the Health and Social Care Information Centre (HSCIC) which administers the opt-outs from Care.data. The ICO says that data subjects' personal data has been processed unfairly, outside of their reasonable expectations.

In January 2014 a leaflet was sent to all households in England offering patients the chance to opt out of their personal confidential information being shared by HSCIC for purposes other than direct care, known as the 'Type 2 objection'. Patients were instructed to inform their GP if they decided to apply the Type 2 objection to their own personal confidential data.

HSCIC has a duty to share some patient information with third parties for the purposes of direct care. For example, HSCIC may share information to aid nationally approved screening programmes, such as NHS breast screening, and so the Type 2 objection will not be applied in these cases.

However, for legal and technological reasons HSCIC was not able to collect, record or implement the Type 2 objections registered by patients with their GPs. This has resulted in Type 2 objections not being implemented for approximately 700,000 patients, the ICO says.

By not being able to collect, record and apply the Type 2 objections it appears that the HSCIC has shared patients' data with other organisations against their wishes. The ICO is also concerned about the way in which HSCIC has communicated with the general public about this matter.

- *See the Undertaking at https://ico.org.uk/media/action-weve-taken/undertakings/1623957/hscic-undertaking-20160419.pdf*

Around 1 in 45 patients opt-out from Care.data

More than one million patient opt-outs have been received for the NHS Care.data scheme, the Health and Social Care and Information Centre (HSCIC) says. The individuals have opted out from sharing the information that identifies them outside of the HSCIC for purposes beyond direct care.

Since early 2014 patients have been able to register two types of opt-out with their GP practice in order to express preferences about the way their personal confidential information should be used for purposes beyond their direct care. These have been more commonly known as 'Type 1' and 'Type 2' opt-outs. Care.data has been criticised for not organising a patient consultation over how their personal data could be shared with the private sector organisations.

- *See http://www.hscic.gov.uk/catalogue/PUB20527*

book review

SWIPED – How to protect yourself in a world full of scammers, phishers, and identity thieves
by Adam Levin

Adam Levin, a long-time consumer advocate and ID fraud expert, describes in this book how to keep hackers, phishers and spammers from becoming your problem.

Swiped is a story about surviving the identity-theft epidemic. This is not a book for lawyers, but it is a practical guide to keeping data safe, and a reminder of why we need to do this at all. There is an overview at the beginning which should be required reading for anyone handling data, either their own or their company's. If every employee were to read the case studies of lives ruined by criminals, or by carelessness, the need for security training would be entirely obvious.

The chapter "Business Considerations Culture eats Strategy" is particularly interesting. Levin cites many examples of institutions' failures to grasp the way that identity thieves work in their hunt for vulnerabilities. Levin quotes the FBI that there were probably fewer than 10% of companies which could have prevented an attack like the one on Sony. The lesson Sony was forced to learn was that security had to be practised at the level of each individual employee, including what you can and cannot say in an email, when to use encryption, how to handle files of former employees and so on.

Levin cites with approval Dr Ann Cavoukian's "7 Principles for Privacy by Design" which can easily be adapted for his "Security by Design concept of three M's: Minimize your Risk of Exposure, Monitor your Security, Manage the Damage".

The chapter on legal initiatives in the US criticises lack of federal oversight when it comes to consumer-related security. Levin searches for a solution that could benefit business, consumers and the government, and finds one in legislation that has been on the statute books since 1988 – the Schumer Box. This legislation requires the small print of credit card agreements, to appear in easy to understand format on every agreement. Levin suggests that a "data breach disclosure box" would encourage organisations to improve their breach-preparedness plans so that they can notify consumers sooner and provide a more transparent and empathetic response. A company can demonstrate, in this way, that it is aiming to do everything it can to help consumers, strengthen its defences and maintain data according to cutting edge standards.

A thoughtful book for the general reader, consumer-orientated, covering the basics in an easy to read style, with a comprehensive index, a glossary of scams and useful tips to avoid becoming a victim.

Reviewed by Merrill Dresner

Published by www.publicaffairsbooks.com, £16.99 ($24.99), ISBN: 9781610395878. Publication date: 24 November 2015.

Latest FOI disclosure logs now available

The Department for Culture, Media & Sport has published disclosure logs for Freedom of Information releases between October and December 2015. They reveal which cases have been refused in part, and which have been responded to in full.

The ICO recommends publishing as much information as possible through publication schemes. The seven classes of information that are recommended are broad and include headings like 'Who we are and what we do' and 'The services we offer'. The classes cover all the more formal types of information organisations hold, such as information about the structure of the organisation, minutes of meetings, contracts, reports, plans and policies. Public information should be made available unless there is good reason to withhold it, and the Act allows it, the ICO says.

- *See www.gov.uk/government/publications/disclosure-logs-for-freedom-of-information-releases-between-october-december-2015*

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
You will be sent the PDF version of the new issue on the day of publication. You will also be able to access the issue via the website. You may choose to receive one printed copy of each Report.

3. E-Mail Updates
E-mail updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

4. Back Issues
Access all the *PL&B UK Report* back issues since the year 2000.

5. Events Documentation
Access UK events documentation such as Roundtables with the UK Information Commissioner and *PL&B Annual International Conferences*, in July, Cambridge.

6. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"I particularly like the short and concise nature of the *Privacy Laws & Business Reports*. I never leave home without a copy, and value the printed copies, as I like to read them whilst on my daily train journey into work. **Steve Wright, Chief Privacy Officer, Unilever**"

Subscription Fees

Single User Access
UK Edition **£400 + VAT***
International Edition **£500 + VAT***
UK & International Combined Edition **£800 + VAT***
* VAT only applies to UK based subscribers

Multi User Access
Discounts for 2-4 or 5-25 users – see website for details.

Subscription Discounts
Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.
Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

International Postage (outside UK):
Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30
Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

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

Privacy Laws & Business also publishes the International Report.
www.privacylaws.com/int