ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

ICO's Denham: Children's code and Adtech key pieces of work

As the ICO issues its AdTech report, a response to the government's Online Harms paper and prepares the Children's code, the regulator is firing on all cylinders. By **Laura Linkomies**.

Speaking at PL&B's 32nd Annual International Conference on 2 July, Information Commissioner, Elizabeth Denham, said that with the GDPR now in force for more than a year, it is time to talk about what the law means in practice. Denham said that the implementation of the GDPR requires both systemic and structural changes.

The session was chaired by Christopher Millard, Professor of Privacy and Information Law at Queen Mary University of London,

Continued on p.3

Real Time Bidding – 'unfair disproportionate, intrusive'

The ICO says stakeholders have six months to review their adtech practices on consent, transparency and accountability. By **Mark Sherwood-Edwards** of This is DPO.

In its recent paper, *Update report into adtech and real time bidding* (20 June 2019), the ICO has set out a biting criticism of how real time bidding (RTB) currently operates in the UK. The phrase *disproportionate, intrusive and unfair* occurs three times, and intrusive on its own is used an additional three times. The paper is not intended as formal guidance, but it gives a clear sense of direction. The ICO also adds that the issues it raises in this paper are not the only concerns it has with programmatic advertising.[1]

Continued on p.4

www.privacylaws.com

Subscribers to paper and electronic editions can access the following:

- Back Issues since 1987
- New search function
- Materials from PL&B events
- Videos and audio recordings

See the back page or **www.privacylaws.com/subscribe**

To check your type of subscription, contact kan@privacylaws.com or telephone +44 (0)20 8868 9200.

Issue 104 **July 2019**

PL&B Services: Publications • Conferences • Consulting • Recruitment
Training • Compliance Audits • Privacy Officers Networks • Roundtables • Research

UNITED KINGDOM
report

ISSUE NO 104 JULY 2019

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Mark Sherwood-Edwards
This is DPO

Lore Leitner and Josephine Jay
Wilson Sonsini Goodrich & Rosati

Dr Oliver Butler
Oxford University

Robert Waixel
Anglia Ruskin University

Barry Murphy
Vodafone

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
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

Copyright: No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior written permission of the publisher.

© 2019 Privacy Laws & Business

comment

Pan-European enforcement to start and finish for the UK?

The ICO's report on Adtech and real-time bidding systems calls for industry to react before there is another review in six months' time (p.1). To date, we have seen complaints in at least seven European jurisdictions regarding Adtech. The ICO is cooperating with European colleagues on this subject, and also acted as Lead Supervisory Authority under the One Stop Shop procedure in issuing its intent to fine Marriott Inc and British Airways (p.6). It is a shame if this formal cooperation channel will come to an end with the UK's Brexit. At our summer conference in Cambridge, Andrea Jelinek, Chair of the European Data Protection Board was not able to say whether UK would have an observer status at the Board, but the issue will be discussed she said.

Speaking at the same conference, Elizabeth Denham, Information Commissioner, said the ICO will be busy in the courts in the next 12 months pursuing its enforcement cases. Another area of focus is the Age Appropriate Code, which the regulator is required to issue under the UK DP Act 2018 (p.1). Its wide scope means that many organisations that would not instinctively think of being caught may nevertheless be affected (p.7) even if their products and services are not specifically addressed to young people. This piece of work, as well as Adtech, may have global implications as regulators have not previously concentrated on these areas.

UK Brexit options remain open but the The Department for Digital, Culture, Media & Sport is busy preparing documentation for a future adequacy application to make it as easy as possible for the EU to come to a decision. The UK government's view is that the UK data protection regime is even stronger than the GDPR (p.12).

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.

Denham ... from p.1

who asked Denham to identify her main areas of work for the year ahead. Denham said that there will be a great deal of work to follow up the investigation started with her Democracy Disrupted report into political influencing. She thought that this is a wider question that requires an update of UK electoral laws as political campaigning takes place all year, we now know of foreign interference, data harvesting, etc. A final report based on the ICO's forensic investigations will be issued in the autumn.

The other major area of work is looking into data ecosystems. The ICO has just issued a report on AdTech and real time bidding (see p.1). "This is a complicated ecosystem with extremely wide implications. We need to look at the ecosystem as a whole and include all players giving industry time to respond to our concerns. At the same time, we need to enforce the law. Before issuing the AdTech paper we talked to 100 people representing the industry and lawyers to get their views. Based on the feedback received, we believe that the industry recognises the need for change."

"We need to be outcomes based. We cannot solve the industry's problems, and we are not an economic regulator. We have also received criticism about giving industry time to sort this issue out. The ICO chose real time bidding as an example, as much special category data has been shared without consent. The industry now has six months to respond to our concerns."

Millard asked what happened if after six months the industry has made an effort but the general public does not support this approach as they may like the benefits that innovative means of advertisement delivery can provide.

Denham said that the next step would be a broader industry approach. There are many design orientated companies, and the GDPR is putting incentives in place to use Privacy by Design, she said. "That's what GDPR is supposed to do."

Millard said that there is much concern about protecting individuals from online harms, and the government has recently issued a wide-reaching White Paper on Online Harms. What is the ICO's role in this field? Would the ICO like to become a regulator for Online Harms?

Denham said that the UK government is leading in this area, and many other jurisdictions such as France and Germany are now also looking at these issues but the UK paper was the first one issued. The UK government proposes a new regulator for this field. The ICO, in its response of 2 July to the government's paper, says that there is no need for a new regulator. Regulation of harmful content online would be best to be assigned to an existing regulator who already has experience in this area, for example Ofcom.

"It should not be the ICO. The work the regulator needs to do is not in our fundamental role, even if we have an active role to play in content moderation."

Millard pointed out that the government is suggesting an extremely wide scope, for example misinformation, and hurtful comments online would be included. "The ICO has used this type of expansion as well – I am therefore concerned about the impact on freedom of the press and freedom of speech."

Denham said that there is much online information that is not illegal but is clearly harmful. Online shaming is serious, but the UK's defamation laws may not address that. It is important to tackle this problem without compromising freedom of information.

Millard: "Have you increased protection for children?"

Denham: "We are required to write a childrens' code under the UK DP Act 2018. It will have design considerations, so using Privacy by Design. The draft code is out for consultation now, and there is much support for it but also push back from the entertainment and media industry."

Denham said that the ICO is not calling for age verification but design solutions. "Many larger providers can estimate children's age already based on the information they have. They do not need to have a verification system. That would collect too much verification

ICO'S RESPONSE TO THE PAPER ON ONLINE HARMS

A summary of the Information Commissioner's response to the Department for Digital, Culture, Media & Sport consultation on the Online Harms White Paper:

- The impact of online harms is an issue of significant public concern. It is essential that we have regulation that makes a real difference, but also remains proportionate so that people are able to continue to enjoy the real benefits of the Internet.
- How to regulate harms on the Internet is one of the most complex and challenging issues of our times. It requires innovative solutions and an approach that ensures we can continue to balance competing rights in a democratic society.
- It is essential that the full breadth of Internet harms is considered in the round, both at an individual and societal level. This includes electoral interference and greater transparency in online advertising.
- Data protection regulation needs to be seen as part of the wider ecosystem of regulating the Internet and should not be positioned separately. It is the personalisation of data that is driving the delivery of content online.
- Given the need to act swiftly, it makes sense for an existing regulator who already has experience of content regulation to take on the new regulatory role outlined in the White Paper.
- This should be accompanied by a strategic coordinated approach to regulation – chaired by the regulator with responsibility for online harms but involving all the key regulators in the space of Internet regulation.
- The proposed duty of care is an important part of the solution – but it is not a quick solution and will need to be backed by appropriate sanctions and powers.

Denham says in the response that she is "surprised and disappointed at the lack of engagement within the White Paper with the societal harm of electoral interference and the need for greater transparency in online political advertising and micro targeting. If left un-addressed, this [lack of transparency] risks undermining the fabric of our democracy. I therefore welcome the Government's commitment to launch a consultation on electoral integrity that I understand will include consideration of recommendations for increasing transparency on digital political advertising."

See ico.org.uk/media/about-the-ico/consultation-responses/2019/2615232/ico-response-online-harms-20190701.pdf

information. We try to change the way services are provided for children."

She underlined that the Internet was designed for adults and to gather as much personal data as possible. It is therefore imperative the we now look at these practices to make the Internet safer for children.

Q AND A WITH THE INFORMATION COMMISSIONER

Now that you have powers to conduct non-consensual audits, have you used your new audit powers?
Denham: "Yes we are making good use of them – we have audited many political parties and data brokers, credit reference agencies, and also issued assessment notices on companies we are taking to court."

Denham said that around 60 people now work on audits at the ICO.

With regard to harassment and taking down content, how do you ensure that this work does not lose momentum at the ICO with a new regulator coming in?
Denham: "The Right to be Forgotten (RTBF) is critically important to the ICO, but the government proposal is so much broader than that."

What are you looking for with the new AdTech paper? A complete fix?
Denham: "I am not looking for a complete fix but we need a change. I am confident that we will get there, as the 100 or so industry representatives and lawyers we talked to before issuing the paper recognise that something needs to change."

In the Age Appropriate Design Code, why is the age limit for a child set at 18?
Denham: "Under the GDPR the age limit is 13 when offering an information society service to children. The definition of a child is difficult; our draft code refers to 18 as this was the decision by Parliament."

Eighteen is in accordance with the UN Convention on the Rights of the Child which defines a child as everyone under 18 unless, "under the law applicable to the child, majority is attained earlier" (Office of the High Commissioner for Human Rights, 1989). The UK has ratified this Convention.

What are the priorities at the ICO for the next 12 months?
Denham: "The next challenges will be the laying of the Age Appropriate Code (children's code) before Parliament and working with companies to implement it. We will also be in court a lot as a result of our enforcement cases."

Denham said that the cost of litigation is considerable to the ICO and it is going to ask for extra funding from Parliament as the large multinational companies have huge resources.

Real Time Bidding ... from p.1

Although the ICO has stated that it will take another six months to investigate further, it is already clear that it will intervene. The ICO's paper, and its forthcoming intervention, are likely to have a substantial impact in the programmatic industry in the EU and the US. It is no exaggeration to say that the ICO's intervention is likely to have a bigger impact on this industry than the GDPR. To give some idea of scale: the worldwide spend on programmatic advertising is expected to reach US$98bn in 2020, representing 68% of total expenditure on digital media advertising.[2] In Europe, the UK is by far the largest market, followed by Germany and then France (approximately US$15bn, US$8bn, US$4bn, respectively, in 2018).[3]

The ICO's activity can be traced back to investigations led by the CNIL in the last few years, culminating in *Vectaury* in October 2018[4] and the subsequent €50m fine of Google in January 2019.[5] In those cases, the CNIL had exposed how companies improperly obtained personal data and then traded that data amongst each other as part of RTB. The CNIL has been particularly critical of the implementation of consent as a lawful basis (generally improperly carried out), a general laxity around the handling of personal data (Vectaury had been ordered to delete 67 million user records collected from RTB), and the use of contractual warranties amongst the companies involved in lieu of consents directly obtained from the data subject.

Against that background, it would have been very difficult for the ICO to ignore the issues raised by RTB. Earlier this year the ICO held a workshop with members of the industry to gather information on how the programmatic advertising worked in practice, and the recent paper is one of the results of that workshop (*PL&B UK* March 2019, p.1).

In its paper, the ICO reached the following conclusions:

1. The intrusive nature of RTB meant that, under the GDPR, the only lawful basis available is consent. Sections of the industry had argued that legitimate interest was a viable basis: the ICO strongly disagreed.
2. Some of the data being processed was special category data: clearly this required consent.
3. Lack of transparency was also a concern. Not only lack of transparency in the usual sense that the purposes for which the data to be used were insufficiently described, but also in the sense that – because the RTB ecosystem involved more than 1,000 players which would participate, or not participate, on an ad hoc basis – it was impossible for users to get any real idea of who their data would be shared with.
4. The industry was set up so that each player claimed to be a controller: that then imported the accountability principle. The accountability principle required that you were able to demonstrate that you actually had consent: it was enough to show that you were part of a contractual chain of warranties, each referring back to the original company that had collected the consent.
5. There was insufficient discipline around the handling of personal data. The nature of RTB was that individuals' profiles were freely traded amongst participants in the RTB process, with little regard to who received the data, its subsequent deletion, and so on.
6. In the ICO's view, RTB was both large scale and high risk: it therefore met the criteria for mandatory DPIAs. DPIAs were few and far between in the RTB world.

 © 2019 PRIVACY LAWS & BUSINESS

Consent and legitimate interest

The ICO made the point that all data collection in RTB started with cookies and that the placing and use of cookies for marketing and advertising – being clearly non-essential uses – requires consent. The ICO noted that most companies participating in RTB had assumed that rules around cookies (which derive from the E-privacy Directive of 2002) have been subsumed by GDPR. In fact, the contrary was the case: in relation to cookies, the E-privacy Directive (and in the UK, PECR, the law implementing the E-privacy Directive) trumps the GDPR.

Starting with the requirement of consent for marketing and advertising cookies, the ICO went on to conclude that consent was the only lawful basis for RTB under GDPR. Although you may need consent for *some* uses, that does not mean that you need consent for *all* uses. Requiring GDPR consent for *all* data processing that flows from a non-essential cookie might be stretching the need for consent too far. In fact, the ICO seemed unusually inconclusive on this point: "whilst associated processing of personal data may be able to rely on an alternative lawful basis, consent is also the *most appropriate* lawful basis for processing of personal data beyond the setting of cookies." [emphasis added]. "*Most appropriate*" does not sound like a legal conclusion about what the GDPR allows or does not allow.

The key problem here is that the E-privacy Directive/PECR and the GDPR simply to do not fit together. To give a simple example, PECR requires that the information given for non-essential cookies be "clear and comprehensive". However, presumably this is not the GDPR Article 13 standard which uses 533 words to specify its transparency requirement. The GDPR refers to the need to adjust the E-privacy Directive so that it more closely aligns to the GDPR (Recital 173), but this seem unlikely to happen any time soon.

Transparency and accountability

According to the ICO, although the GDPR allows for privacy notices to specify "recipients or categories of recipients", if the recipient of the data is going to rely on consent as the lawful basis, the identity of the recipients needs to be provided to the individual when his or her data is first collected. Arguably this is a creative reading of the GDPR (consent can be just as freely given, specific, informed and unambiguous in relation to a category, as it can be in relation to an individual) but in practice it is unlikely to make much difference. If participants in RTB are relying on consent, then they must be able to demonstrate that they have consent (Article 7.1). And then, as controllers, they must be able to demonstrate accountability in relation to the data they process – what data they receive, how they hold it, what they do with it, how they protect it. The ICO was far from convinced that most participants in RTB would able to do so.

Special categories of data

RTB uses taxonomies to classify people and websites. Existing classification types include Heart and Cardiovascular Diseases, Mental Health, Sexual Health and Infectious Diseases, Reproductive Health, Substance Abuse, Health Conditions, Politics and Ethnic & Identity Groups, all of which, if used in relation to an individual, reveal special categories of data. The ICO's investigations showed that these taxonomies were used both to determine the advertisements that were served to the consumer and also to determine the advertisements that would appear on a particular website. For example, if the taxonomy showed that users were vegetarians, serving them with an advertisement for cheap beef would be pointless. Equally, it would not make much sense to serve an advertisement for cheap beef to a vegetarian website. The ICO's view was that both these uses, when they involved special categories of data, required consent. While the first usage, based on the taxonomy of a particular person, is clearly processing of personal data, it is hard to see how the latter (a rule matching website types to advertisement types) can be, since the rule exists independently on any particular individual.

However, the ICO's main point is clear: the way that RTB presently occurs is disproportionate, intrusive and unfair. It expects participants, the industry, and in particular the owners of two protocols that allow RTB to take place – the IABs OpenRTB and IAB Europe's Transparency and Consent Framework (*PL&B International* February 2019, p.1); and Google's Authorized Buyers framework – to go back and rethink their whole approach.

> The ICO's paper, and its forthcoming intervention, are likely to have a substantial impact in the programmatic industry in the EU and the US.

Why now?

A key question though, is why now? Why is the ICO carrying out an in-depth investigation of RTB now when RTB has been around for several years? Is it because the previous CNIL investigations had highlighted RTB that the ICO felt emboldened, or was it the arrival of the GDPR which gave it the confidence to take on a whole industry? It is odd to see the ICO so aghast in its report when it must have known that RTB was fairly standard practice. In fact, even in 2011, the ICO guidance on third party advertising stated: "However, using personal data in this way is not intrinsically unfair or intrusive, and the DPA provides various options for processing this information legitimately – i.e. there are alternatives to consent."

There are probably two main reasons. The first is the arrival of the Internet of Things which will multiply hugely the amount of data collected about individuals and allow geographical and cross-device tracking with increased facility. No doubt the ICO felt that, with the horse already half out of the stable, it had to act now, or the horse would be long gone.

Secondly, the ICO has finally come of age. In the space of a few weeks it has decided to take on an industry, and also announced its intention to fine British Airways £189 million and Marriott Hotels more than £99 million, both fines far in excess of any fine it has

previously levied. In the world of data protection, at least in the UK, the centre of gravity has shifted.

Next steps

The ICO acknowledges that RTB is a complex area. It therefore plans to take a "measured and iterative approach" before undertaking a further review in six months' time. However, some kind of intervention seems inevitable. In fact, the report says as much: "We do not think these issues will be addressed without intervention." The most likely outcome is that the ICO will come back with a timetable for action by which it expects RTB players to comply more closely with the GDPR. Whether they will be able to, and preserve existing revenues, is another matter.

AUTHOR

Mark Sherwood-Edwards is Founder of This is DPO, an external DPO service.
Email: mse@thisisdpo.co.uk

REFERENCES

1 "Programmatic" ad buying typically refers to the use of software to purchase digital advertising, as opposed to the traditional process that involves RFPs, human negotiations and manual insertion orders. It's using machines to buy ads, basically. digiday.com/media/what-is-programmatic-advertising/
2 www.zenithmedia.com/65-of-digital-media-to-be-programmatic-in-2019/
3 www.appnexus.com/sites/default/files/whitepapers/guide-2018stats_2.pdf
4 thisisdpo.co.uk/2018/11/27/french-ico-orders-deletion-of-67-million-records/
5 thisisdpo.co.uk/2019/01/26/cnil-v-google-what-google-got-wrong/

ICO intends to fine BA £183 million and Marriott £99 million for GDPR breaches

The ICO issued, on 9 July, a statement of intention to fine Marriott International Inc for a breach of the GDPR. The ICO says that the proposed fine relates to a cyber incident which was notified to the ICO by Marriott in November 2018. "A variety of personal data contained in approximately 339 million guest records globally were exposed by the incident, of which around 30 million related to residents of 31 countries in the European Economic Area (EEA). Seven million related to UK residents."

In the BA case, the fine relates to a cyber incident notified to the ICO by British Airways in September 2018. In this breach, personal data of approximately 500,000 customers was compromised.

"The ICO's investigation has found that a variety of information was compromised by poor security arrangements at the company, including log in, payment card, and travel booking details as well name and address information."

British Airways said: "BA has cooperated with the ICO investigation and has made improvements to its security arrangements since these events came to light. The company will now have opportunity to make representations to the ICO as to the proposed findings and sanction."

The ICO has not issued details on what kind of security aspects the companies should have applied. The regulator acted as the Lead Supervisory Authority in both cases under the GDPR's One Stop Shop provisions.

- *See ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/ and ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-ico-announces-intention-to-fine-british-airways/*

AI, machine learning and device tracking all included in future work plan at ICO

The ICO says that its regulatory priorities include cybersecurity; AI; big data and machine learning; web and cross-device tracking for marketing purposes; children's privacy; use of surveillance and facial recognition technology, as well as data broking; the use of personal information in political campaigns; and freedom of information compliance.

A call for views on the **data sharing code** closed in September 2018, and the ICO is currently considering the views presented to develop a draft code for formal consultation. "We expect to launch that consultation in June 2019 and for the code to be laid before Parliament in the autumn," the ICO says.

A call for views on the **direct marketing code** closed in December 2018 and the ICO is currently considering the feedback. This will inform a draft code. A formal consultation is expected this summer with the view to finalising the code by the end of October. It may be necessary to further review the code once the EU e-privacy regulation is adopted.

A **data protection and journalism code** was subject to an evidence-gathering exercise which closed on 27 May 2019. The ICO is now developing a draft code for formal consultation and expects to lay the code before Parliament in the summer.

The ICO has proposed a code of practice on **political parties and data protection** and hopes it will be placed on a statutory footing. The ICO is now developing a draft code for formal consultation which is likely to be launched in July.

 © 2019 PRIVACY LAWS & BUSINESS

The ICO's Age Appropriate Design: Draft Code of Practice

The code applies also to services which are likely to be accessed by children. **Lore Leitner** and **Josephine Jay** of Wilson Sonsini Goodrich & Rosati examine the implications.

In April 2019, the ICO released its draft code of practice on Age Appropriate Design (the Code),[1] intended to regulate the provision of online services likely to be accessed by children. As the Code is mandated under the UK Data Protection Act 2018 (the DP Act)[2], this is a statutory code, and not simply advisory. Although a breach of the Code is not directly actionable, compliance with the Code is compulsory in that the Commissioner must take the Code into account when considering whether an online service has acted in accordance with both GDPR and the Privacy and Electronic Communications Regulations.[3]

The ICO has already released guidance on the processing of children's data under the GDPR, in the form of its "Children and the GDPR" guide.[4] Other regulators have also demonstrated similar interest, including the Irish supervisory authority in its public consultation on the processing of children's data and their rights as data subjects.[5] The UK Code, however, is the first attempt by any data protection regulator to offer detailed practical guidance on how the special status afforded to children as vulnerable data subjects is translated into the online space.

The public consultation for the Code closed on 31 May 2019 and the Code is expected to go live, reflecting any amendments resulting from the consultation, by the end of 2019. In this article, we examine the Code's scope, and take a high-level look at the framework introduced by its 16 "standards". This article also considers the Code's broad scope and thus its potentially problematic nature, and the impact it could have on online service providers in the EU and beyond.

Application of the Code

The Code applies to all processing of personal data within the scope of the DP Act. In particular, this means that the Code applies to online services based in the UK, and to online services based outside of the UK to the extent personal data are processed in the context of a UK establishment. The Code also applies to online services not established in the UK (unless they benefit from having a lead supervisory authority in another EU country) to the extent the online services are offered to users in the UK, or the behaviour of such users is monitored. However, the ICO has made it clear that it expects this to become an international benchmark so organisations to whom the Code is not directly applicable should take note.

The ICO defines "online services" as any online products or services that process personal data and are likely to be accessed by children (a child being anyone under the age of 18) including applications, websites, search engines, community environments, programs, games, and specifically including connected toys or devices.[6] This arguably goes over and above what is required by the GDPR, which simply references "services offered directly to a child"[7], indicating an applicability more akin to that seen in the US with the Children's Online Privacy Act (COPPA). The Code, however, not only applies where the service is designed for and aimed specifically at children, but also where it is simply likely to be accessed by children. This significantly broadens the scope of the Code, and potentially creates an uneven level playing field as services which have never taken children into account will have a large divide to bridge.

If a company believes its online service is exempt from the Code by virtue of it only being accessed by adults, it should be able to demonstrate that this is the case, and the best way to do this is to implement a robust age-verification mechanism into its service. The Code does not specify what robust means, but makes it clear that self-declaration alone is unlikely to be sufficient. Alternatively, adult-predominant access can be demonstrated by market research or current user demographics. If, at any point in time, however a company knows that a significant number of children are using its services, the Code will apply even if age verification is in place or market research suggests otherwise.

The Code

Children merit specific protection under the GDPR.[8] Therefore, the Code is intended to provide practical steps on how to design appropriate products for use by children, and sets this out in relation to 16 "standards of age-appropriate design" (the Standards), all of which must be complied with.

Age Ranges: Many of the Standards are built on the requirement to provide online services in an age-appropriate manner, which means that they need to be tailored according to different age-groups.[9] As a guide, the Code identifies five groups within the broader children category (the Age Ranges): these are 0 to 5 years, 6 to 9 years, 10 to 12 years, 13 to 15 years and 16 to 17 years. Companies who do not know the relevant age range of their users must apply the Code's standards to all users. Furthermore, unless a company can clearly demonstrate that its user base is likely to consist only of adults, the Code recommends that the Standards are applied to all users by default, with adults able to opt out of the specifically designed app or service via robust age-verification. According to the ICO, this approach should be followed to dis-incentivise children lying about their age to access services. Companies can also then rely on this age-verification to cater to each individual Age Range. Of course, it remains to be seen how online service providers will and can implement the Age Range specific requirements. Doing so could be very costly and consequently only an option for the larger

players, thereby creating a significant barrier to entry into the market for children-directed online services.

Bolstering existing GDPR provisions: A number of the Standards mirror and expand upon already existing GDPR requirements.

The requirement for transparency[10] is reiterated: privacy information and terms must be concise and prominent with the language tailored to suit the relevant Age Ranges, using just-in-time notices where appropriate.[11] The information should be presented in such a way that will appeal to each age range, for example, via the use of graphics or cartoons. Full guidelines for each Age Range are included in the Code. In addition, companies should implement prominent and accessible tools – again tailored to reflect different Age Ranges – to help children exercise their data protection rights.[12]

The Code also discusses data minimisation,[13] clarifying that companies should only process the minimum data required to provide the elements of the online service with which the child is actively and knowingly engaged, and children should be given clear and separate choice over such processing.[14] . In addition, the ICO confirms that a Data Protection Impact Assessment must be undertaken where services are provided to children, to ensure compliance with the Code, assessing and mitigating risks for each Age Range.[15]

Finally, the Code calls for governance and accountability[16] emphasising the importance of supporting and demonstrating compliance with the Code, including the provision of training. The ICO will at any time be able to ask for evidence of compliance with the Code.

Privacy by Default: Many of the Standards confirm that settings for children are to be set to high privacy by default, in line with Article 25(2) GDPR.[17] Data use should be limited to that which is essential for the provision of the online service unless a child chooses otherwise, or the service provider can demonstrate a compelling reason to do otherwise while taking into account the best interests of the child. This includes limiting sharing of data with third parties (e.g. for advertising purposes), switching geolocation options off, providing a clear sign when a user is being tracked, and turning off profiling. Separate privacy settings for each element of the foregoing should be provided, and switched off by default, with age-appropriate just-in-time notices provided prior to the child switching them on.

The Code makes it clear that "nudge" techniques to encourage the child to opt in to the lower privacy options should not be used. These prohibited techniques include using language to make the lower privacy setting more appealing, and the use of larger more "clickable" buttons to move away from the default.[18] The Code in fact actively encourages using "nudge" techniques to urge the child to stick with the higher privacy settings.

Protecting the welfare of the child: The Code introduces a general obligation for online services to have the best interests of each individual child as a primary consideration.[19] In reality this means that it is unlikely that, where they are incompatible, the commercial interests of a company will outweigh a child's right to privacy. Online service providers must take steps to keep children safe from exploitation and protect and support their physical and mental wellbeing, as well as their views and identity.

Children's data must not be used in ways that are detrimental to their wellbeing, or that go against industry codes of practice or other regulatory provisions and government advice, including the Committee of Advertising Practice guidance, and guidance on limiting addictive screen behaviour (i.e. the use of continuous scrolling and auto-play features).[20] An online service provider's own published terms, policies and community standards must also be actively adhered to, to ensure that a user's reasonable expectations when they use a service are met.[21] Where profiling is switched on, the child must be safeguarded from content that could result in harm. The online service provider is responsible for any content that it "feeds" to the child as a result of profiling.[22] This means that online service providers that recommend content based on a child's previous interactions have a greater responsibility for that content, whether or not it is user generated, than the content it simply provides a platform for, and that a child actively seeks out for itself.

In practice, given the broad application of the Code, these Standards are quite difficult to implement. Many online service providers have AI algorithms which push users, e.g. viewers of videos, to the extreme end of the spectrum in terms of content. Such services may not be directly aimed at children but children may be accessing the services nonetheless, and filtering out children's data requires a large number of technical adjustments (if not a completely separate service or app).

The role of parents: Parents (or guardians) have a part to play where the data of children is involved. Their role should vary depending on the Age Range of each child. Where younger children are involved for example, alternative versions of the transparency information for parents should be provided.[23] This will more generally allow parents, and children, to make informed choices about what online services their children access.

Parental controls should be built-in, allowing parents or guardians to place limits on a child's use of the online services.[24] The Code gives examples of tools to set time limits and restriction of the service, including purchases. These, and tools to monitor online activity and physical location, can help to protect the child's best interests, but may impact the child's right to privacy. To address this, the Code obliges online service providers to make it clear when parental monitoring and tracking are in place. This should be called out in any transparency notices, but the Code also recommends the display of a clear symbol when such a parental tool is active.

The Code reiterates the Article 8 GDPR rule on parental consent – if a child is under 13 and information services are offered directly to them, where consent is the legal basis relied upon, reasonable efforts to seek parental consent must be made. What steps are taken to verify age and parental authority depends on the impact of the processing. The Code does not add any additional guidance as to what services are offered directly to children in this context and the steps that are reasonable to take.

 © 2019 PRIVACY LAWS & BUSINESS

What next?

The consultation period for the Code closed on 31 May. Amendments will no doubt be made, but we expect that the substance of the Code will make its way into the final version. In the draft Code, the ICO makes it clear that use of children's data is a regulatory priority so once the final version of the Code comes into force, enforcement is likely to follow close behind.

Companies which may be impacted by the Code should undertake an analysis as to whether their services are likely to be accessed by children. To argue that they are not will require strong documentary evidence based on market trends and existing demographics, and such evidence takes time and resources to put together. Those who will be in scope should begin to manage internal expectations regarding potential product and policy changes. It would, however, be prudent to wait until the final code is published before making seismic changes.

Companies which are not directly impacted (e.g. online service providers with a non-UK lead supervisory authority) should continue to monitor international reactions to this Code and its final version to see if something similar is likely to be introduced in other jurisdictions. In the EU both France's CNIL and Ireland's Data Protection Commission have indicated that the treatment of children's data will be a priority. This trend towards greater protection of children can also be seen outside of Europe, with China affording them particular protection as part of its newly introduced regime,[25] and COPPA investigations ramping up in the United States. In light of this global trend, it is likely that regulators in the EU and beyond will continue to influence, learn from and potentially cooperate with, each other as they tackle this common concern.

AUTHORS

Lore Leitner is Of Counsel, and Josephine Jay an Associate at Wilson Sonsini Goodrich & Rosati, London. Email: lleitner@wsgr.com

REFERENCES

1 ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/age-appropriate-design-a-code-of-practice-for-online-services/
2 Section 123, DP Act
3 Section 127, DP Act
4 ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/
5 www.dataprotection.ie/sites/default/files/uploads/2018-12/DPC_Childrens Rights_2019_English.pdf
6 Standard 14, the Code
7 Recital 38, GDPR
8 Recital 38, GDPR
9 Standard 2, the Code
10 Articles 5(1)(a), 12, 13 and 14, GDPR. Article 12(1) specifically calls out that this principle particularly applies in relation to information addressed to a child
11 Standard 3, the Code
12 Standard 14, the Code
13 Articles 5(1)(c) and 25, GDPR
14 Standard 7, the Code
15 Article 3, GDPR and Standard 15, the Code. The ICO has already separately published guidance saying a DPIA should be conducted where online services are offered directly to children.
16 Articles 5(2), GDPR and Standard 16, the Code
17 Standards 6, 8, 9 and 11, the Code
18 Standard 12, the Code
19 Standard 1, the Code
20 Standard 4, the Code
21 Standard 5, the Code
22 Standard 11, the Code
23 Standard 3, the Code
24 Standard 10, the Code
25 As seen in China's Personal Information Security Specification which supplements its 2016 Cyber Security Law.

Elizabeth Denham speaks at G20 side event

At a G20 side event in Japan, Information Commissioner Elizabeth Denham spoke about different data protection legal systems and stressed that we can acknowledge and respect the differences and find practical ways to bridge them.

"The EU's adequacy process is one approach to achieve interoperability; it has been used successfully to find common ground in legislative approaches as diverse as that of New Zealand, Israel and Japan. The GDPR sets a high bar in terms of data standards, and that bar might seem quite prescriptive for some. But, as an approach, it has achieved trust for European residents' data processed in adequate jurisdictions. But it cannot be an exclusive tool," Denham said.

"Japan and the EU struck a new path in the mutual recognition of each other's laws. Japan could show us the way as a bridge between APEC and EU systems. There is further work for governments to do to consider the merit of a wider application of such an approach – that could include codes, standards and certification systems that allow data transfers with trust."

"The UK will play its part in this, post-Brexit. The UK government is committed to retaining high data protection standards - the GDPR, which has been copied over in full in the exit legislation. And after Brexit, the UK will operate its own transfer regime, including effective trust-based controls for international transfers."

She said that cooperation between Data Protection Authorities is also very important.

"That means trusting each other's views on issues and cases. What we really need to share are lines of inquiry, our analysis of the issues, and the tactics we are adopting in our investigations. This will minimise duplication of investigatory effort and speed up our inquiries. And for businesses - provide more consistency in how they are being regulated by us."

• *See ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/g20-side-event-international-seminar-on-personal-data/*

Data transfers constrained by out-of-date Model Clauses

The EU's Model Clauses need a GDPR update and new European Data Protection Board guidance on international transfers is required. **Tom Cooper** reports.

Transferring personal data outside the European Economic Area (EEA) presents many practical challenges and legal "grey areas". When moving data to jurisdictions not considered "adequate" by the EU, Binding Corporate Rules (BCRs) – one option – are time-consuming and resource-hungry, while the standard Model Clauses currently have large gaps and lag behind legislative and technological change. Brexit will add a further layer of complexity.

A session at *PL&Bs* 32nd Annual International Conference – chaired by Rob Sumroy, co-head of data privacy, at Slaughter and May – tackled some of these issues, coining the word "Dexit" in recognition of the times through which the UK is passing.

Chapter 5 of the EU General Data Protection Regulation[1] governs transfers outside the EEA. Rebecca Cousin, the other co-head of Slaughter and May's privacy practice, emphasised that the mechanisms operated as a "waterfall". If an adequacy decision is not in place, then appropriate safeguards could be considered – BCRs or Model Clauses. "Only then are you allowed to move on and consider the derogations," she said. "I'm sure, like us, you have discovered many practical challenges," she told the audience of privacy professionals and regulators at St John's College, Cambridge, on 1 July.

Intra-group 'Dexit'

The first case considered was an organisation with UK and non-EEA subsidiaries and with the UK subsidiary having both UK and US offices and a single employee in Australia. BCRs are designed for this situation but time and cost deter many organisations. Quoted time frames for regulatory approval vary from six months to four years. "It is really down to time and cost," Cousin said. "We still see most companies going down the Model Clauses route and incorporating those into their Intra-Group Agreements (IGAs)."

The future of the current Model Clauses is uncertain as they face a challenge in the Court of Justice of the EU (CJEU), with the hearing set to begin on 9 July 2019[2] but companies are generally taking the view that they will deal with any fallout from this if and when that arises.

Transfer between branches within the same subsidiary throws up a few issues with Model Clauses. Under UK law, and in many jurisdictions, a legal entity cannot sign a legitimate contract with itself. So Model Clauses signed with another branch within the same legal entity would not, technically, be enforceable.

The ICO guidance from 2019 offers a "pragmatic solution", Cousin said. According to the guidance, she said, "the only transfers that fall within Chapter 5 are transfers from the employees of one entity to employees of another legal entity. So you can transfer data from the UK office to the US office of the same legal entity without having to put further steps in place."[3] This is potentially a "very helpful approach", in practice.

The GDPR bubble

The session continued with a discussion about the concept of the GDPR bubble. This stems from the ICO guidance that transfers of personal data to entities to which the GDPR applies are not restricted, even if the entity is outside the EEA.[4] A US organisation offering goods or services or monitoring behaviour within the EU, for example, would fall within the scope of the GDPR's extraterritorial provisions. "It is important to remember that not all processing will be subject to the GDPR. The extraterritorial provisions, when they apply, will only apply in the context of that monitoring or offering goods and services. It is not a complete *carte blanche*," Cousin said.

This interpretation is being discussed by the European Data Protection Board (EDPB) but the speakers considered that it will likely be a challenge to get regulators from all Member States to support this approach.

Cousin wondered what the future might bring: "Even if the regulators were to get happy with this, what about the privacy activists. Why wouldn't this be challenged?"

Dexit by processor

The GDPR has thrown up a new challenge for UK processors transferring data to a US controller, as data processors now have direct obligations imposed on them. "The basic problem is that there aren't any standard clauses to deal with this relationship," Cousin said. "The DPAs know this is a challenge and we are told the EDPB is discussing it."

This is a grey area where EU guidance is awaited. Approaches discussed by the panel included somehow identifying an EU controller, squeezing into a derogation or looking to bespoke approved clauses.

Onward transfers under Model Clauses

Where a restricted transfer takes place under Model Clauses, say to the US, and the US entity needs to pass it on to, for example, a US law firm, the restrictions on onward transfers are more limiting than under the GDPR in general. Cousin explained that the derogations under the GDPR are not replicated in the Model Clauses. In this example, the US entity cannot therefore use the legal claims derogation to transfer the data to the US law firm. In comparison, if the data was transferred directly from the EEA to the US law firm that would be an option.

"The real solution is that the Model Clauses, when they are updated for the GDPR, should take a different

 © 2019 PRIVACY LAWS & BUSINESS

approach. It is time for a refresh there. But I query if there will be one, as it is not just a change to reflect the GDPR, but a wholesale change to what has gone before," Cousin said.

Sub-processors

Onward transfers to sub-processors from processors are similarly problematic. There are no Model Clauses available, "even though for years we have known we could do with them," Cousin said. "What we normally see people doing is having the processor sign the Model Clauses between the controller and sub-processor on behalf of the controller. As the processor, you do not want to have to keep going back to a controller saying I want to appoint another sub-processor."

Brexit

After leaving the EU, the UK will have what is essentially a copy of the GDPR with a few tweaks. "Transfers outside the UK [post-Brexit] will be subject to the same raft of provisions," Cousin said.

A UK to EU transfer will be a restricted transfer. If there is a 'hard' Brexit and no transition agreement is in place, the UK government has said it will treat the EU as an adequate destination, Cousin said. "The reverse cannot be guaranteed. There is no guarantee of an adequacy decision. Hopefully we will have some sort of transition period, but we don't know. That is why we are seeing companies starting to prepare with Model Clauses."

For transfers from the UK to the rest of the world, "we want to continue to rely on those adequacy decisions the EU Commission has made," she said. "The UK government has said it is adopting those wholesale. So they can be relied upon."

"The one to watch out for is the EU-US Privacy Shield." The government has said it can be used but the documentation for the US company needs to be checked. The US company must have put protections in place that have to be documented. "If it still says it will apply those protections to EU citizens, without any reference to UK citizens, then you are not going to be able to rely upon it," Cousin said. US companies are meant to be updating their documentation, but this needs to be checked.

For data flows back to the UK, most jurisdictions that have the EU on some form of 'whitelist' have been adding the UK to the list – for example Japan, Argentina and the Isle of Man.

On-screen 'transfers'

The chair, Rob Sumroy, referred to the ICO guidance. If data can only be viewed, and not downloaded or printed – for example in an overseas call centre – would this fall under the transfer provisions?

Cousin responded: "The guidance does specifically say that having access to the data amounts to a transfer. Even though the data isn't moving through any system – it is still a transfer. It doesn't matter that they cannot download or print it. It is still a transfer."[5]

REFERENCES

1 The EU GDPR text is available at eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
2 See curia.europa.eu/juris/document/document.jsf?text=&docid=204046&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6462885
3 "if you are sending personal data to someone employed by you or by your company, this is not a restricted transfer." See the ICO Guidance at ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/ accessed 5 July 2019
4 You are making a restricted transfer if: "…you are sending personal data, or making it accessible, to a receiver to which the GDPR does not apply. Usually because they are located in a country outside the EEA;…" Emphasis added. ICO Guidance *ibid*.
5 ICO Guidance, *ibid*, "The restricted transfer takes place when someone outside the EEA accesses that personal data …"

Upper Tribunal seeks non-legal members

The Upper Tribunal is looking to appoint ten non-legal members to serve as members assigned to its Administrative Appeals Chamber and First-tier Tribunal General Regulatory Chamber (Information Rights) jurisdiction.

The fee-paid non-legal members will sit with a First-tier Tribunal Judge to determine appeals from decisions of the Information Commissioner made under the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Data Protection Act 2018/GDPR. Non-legal members bring an important lay perspective to hearings, the Tribunal says. While expertise in one of the above areas is required, experience in legal work is not.

• *See www.judicialappointments.gov.uk/vacancies/140*

People in the dark about the use of their data

Parliament's Human Rights Committee, made up of MPs and Peers, says, in its inquiry into the right to privacy and the digital revolution, that the vast majority of individuals do not understand what happens to their data and therefore do not give meaningful consent when using online services.

The ICO argues that there is growing evidence that inherent biases are built into algorithms resulting in the risk of discriminatory outcomes. A risk occurs where there is a choice for a data subject between giving consent and having access to a product denied. Where the service is very important to the individual, or the company in question acts as a de facto monopoly, a question arises over how willingly consent can be given, the ICO says.

• *See the latest from the Parliamentary Joint Committee at bit.ly/2JupbbW*

The UK's room for manoeuvre in DP legislation after Brexit

The government is keen to start adequacy talks with the EU and is establishing its future capability to make such decisions. By **Dr Oliver Butler** of Oxford University.

At the 32nd PL&B Annual International Conference *GDPR's Influence Ripples Around the World*, John Bowman, Senior Principal, Promontory, Elizabeth Stafford, Senior Policy Advisor, EU Data Protection, Department for Digital, Culture, Media and Sport (DCMS), and Urs Maurer-Lambrou, Delegate International Affairs, Swiss Federal Data Protection and Information Commission discussed the UK's room for manoeuvre in data protection legislation after Brexit.

Immediately post-Brexit

John Bowman contextualised his comments by recalling the UK Government's approach to GDPR in July 2012, when he was Head of EU and International Data Protection Policy at the Ministry of Justice. The Conservative/Liberal Democrat coalition was clear on the UK mandate, considering the GDPR over-prescriptive and criticising the administrative burden it feared it would impose. The UK government predicted a high cost to GDPR implementation. Bowman asked how accurate that had been in hindsight. Although the UK's preference for a Directive rather than a Regulation had not been realised in the process leading to the creation of the GDPR, the UK had been able to exploit the derogations available to Member States under it in the Data Protection Act 2018.

Post-Brexit, Bowman emphasised the need to maintain UK leadership in the digital economy without being unduly shackled by regulation. Assuming no further delay or the revocation of the UK's Article 50 notice to leave the EU, he explained that there are two potential scenarios.

The first scenario involved the passage of the Withdrawal Agreement. If passed, adequacy negotiations will commence during the transition period. The UK GDPR will apply, preserving the GDPR in UK law subject to changes made by the Data Protection Act 2018 and amendments made by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (DPEC Regulations), made pursuant to section 3 of the European Union (Withdrawal) Act 2018. There is scope to extend the transition period under the Withdrawal Agreement and the Political Declaration promotes data protection and privacy, seeking the maintenance of high levels of mutual data protection. Bowman considered this to be the "easiest scenario", with room for adequacy that would maintain the flow of data.

The second scenario involved a no-deal Brexit. The UK would then have immediate third-country status for the purposes of international data transfers from the EU under the GDPR, and data controllers and processors would have to rely on Binding Corporate Rules, Standard Contractual Clauses or derogations under Article 49 GDPR for transfers to the UK. The EDPB has published an information note on data transfers under the GDPR in the event of a no-deal Brexit.[1]

Bowman questioned whether there would be room for manoeuvre in the future to make the UK more business friendly and to reach out to the outside world as "Global Britain". It would be important to collaborate and develop links internationally.

Adequacy post-Brexit

Elizabeth Stafford observed that it was an "exciting time to be a civil servant" in data protection policy. She had been closely involved in negotiating Title VII of the Withdrawal Agreement, on data and information processed or obtained before the end of the transition period or on the basis of the agreement. Its implementation would preserve continuity while the Department for Digital, Culture, Media and Sport (DCMS) prepared for all outcomes, including working with the ICO on guidance on a no-deal Brexit.[2] She argued that while there was more margin for manoeuvre, there would be "no race to the bottom", as the UK had a long tradition of protecting data and had been a signatory of Council of Europe Convention 108. The UK had achieved its negotiating objectives in the GDPR and had championed and voted for it. National legislation had been passed to align with the EU, with the Data Protection Act 2018 implementing the GDPR and the Law Enforcement Directive. Following Brexit, when the GDPR will not be directly applicable, the European Union (Withdrawal) Act 2018 and DPEC Regulations will ensure that the UK GDPR functions on exit. The UK GDPR maintains data protection standards and obligations, with deficiencies remedied by the DPEC Regulations, for example by changing references to Member States, the EU Commission, and Union law to the UK, the Secretary of State and domestic law respectively.

Stafford argued that this placed the UK in the best possible position for an adequacy decision. The EU Commission's powers to make adequacy decisions would be transferred to the Secretary of State for the purpose of the UK GDPR, so the UK will have its own transfer regime. The DCMS is currently establishing future capability to make such decisions and there is no intention to lower standards. Existing adequacy decisions will be kept under review. The DCMS has been working with Switzerland and others to maintain flows to the UK post-Brexit. The UK's alignment will preserve the UK's adequacy in line with the EU Commission's referential document.[3] This, and the strong record of the ICO, will be used by the UK Government to show that the UK GDPR exceeds essential equivalence, the EU's standard for an adequacy declaration.

Stafford emphasised that historically, the UK had a strong tradition in data protection. The EU Commission would of course have to do its due diligence and so they could not assume adequacy. Both

 © 2019 PRIVACY LAWS & BUSINESS

sides also wanted any adequacy decision to be reliable so that it is not struck down by the Court of Justice of the European Union (CJEU). One conference attendee asked what impact UK surveillance laws will have on adequacy. Stafford argued that there was a need for myth busting on the Investigatory Powers Act 2016. She did not expect that it would be a substantive obstacle, due to the transparency, limits, oversight, safeguards for necessity and proportionality in the legislation. She noted that the UN Special Rapporteur on the Right to Privacy, Joseph Cannataci, had praised the UK for its multiple safeguards.[4]

Transfers between UK and third countries: Switzerland

Urs Maurer-Lambrou added that the Swiss Data Protection Authority would not need to make any immediate changes to its international transfer provisions, as the UK is listed separately as an adequate country. There was not currently any evidence to suggest a change in its status was necessary, although it would be reviewed according to applicable data protection laws in force after Brexit.

Switzerland's legislative process moved slower than some other countries but there was no sign of the "race to the bottom". The 26th Annual Report of the Federal Data Protection and Information Commissioner (now available in French, German, Italian and English) had emphasised the need to move forward and for the Swiss Parliament to advance and pass a GDPR law.[5] The Swiss Federal Council will ultimately decide any future adequacy decisions.

Room for manoeuvre

The panel gave an excellent insight into the UK's room for manoeuvre in the immediate aftermath of Brexit and into the Government's current position on adequacy and UK data protection. That current policy strongly emphasises the importance of continuity and stability in international data flows to the UK and seeks to achieve it through close alignment and an adequacy decision from the European Commission. However, less consideration was given to the UK's room for manoeuvre in the event of a change in Government policy. European Commission adequacy decisions are likely to remain an important part of debates around the future of data protection in the UK and careful attention will no doubt be paid to the review of existing adequate countries. It remains to be seen whether New Zealand, Canada, US or other models of adequacy remain viable and may become attractive alternatives to the UK in the medium to long term.

Such shifts are not impossible. There will be pressure post-Brexit to make the UK more attractive to business investment and a more flexible approach to data protection is likely to be a feature of such pressure in some industries. There will also be those in the UK who look to the UK's extensive administrative datasets in the public sector, especially in health, education and social welfare, to ask whether different data protection rules could allow the potential of those datasets to be more fully realised. However, this does not mean that there will necessarily be a "race to the bottom". There are good reasons to promote data protection to enhance trust and confidence in markets and institutions. However, such market-driven reasons alone might not support a high level of data protection in all sectors of the market.

Stafford's portrayal of the UK's place as a strong and consistent supporter of data protection laws can be questioned, as can the value of such historical claims in predicting future UK policy on data protection, in light of the unpredictability and instability that has followed Brexit. Although current policy is to pursue continuity and stability, will that persist under the next Government or one five or ten years from now? The UK was not an early adopter of data protection laws in the late 1960s and 1970s.[6] The Data Protection Act 1984, implementing Convention 108, was passed more to prevent barriers to the free flow of information, than out of a pioneering commitment to digital rights.[7] The UK Government resisted an expansive scope for the 1995 Data Protection Directive and was subject to a lengthy disagreement with the European Commission over its implementation in the Data Protection Act 1998, which the Commission considered lacking.[8] The GDPR was in turn subject to criticism from the UK for being unduly administratively burdensome. There must be a likelihood of some appetite for a degree of divergence post-Brexit. The question will be what can be done and at what risk to the UK's adequacy in the eyes of the European Commission and CJEU.

A greater degree of divergence is likely in the event of a no-deal Brexit. One reason for this is that much of the disruption and cost to existing businesses, in terms of setting up Standard Contractual Clauses and Binding Corporate Rules, would be experienced immediately preceding and immediately after a no-deal Brexit. Once those costs are fully realised, the attractiveness of adequacy will partially diminish. It is difficult to assess how great the impact of a lack of adequacy will be on UK competitiveness and it remains to be seen whether the European Union's assessment of UK surveillance laws will require any step too great for a future UK Government to accept. However, if the UK becomes unmoored from European data protection, the medium to long term potential for divergence may be more considerable than the room for manoeuvre in the shorter term.

AUTHOR

Dr Oliver Butler is Fellow at Wadham College, Oxford and Research Fellow at the Bonavero Institute of Human Rights, Oxford.
Email: Oliver.Butler@wadham.ox.ac.uk

REFERENCES

1 edpb.europa.eu/our-work-tools/our-documents/drugo/information-note-data-transfers-under-gdpr-event-no-deal-brexit_en
2 ico.org.uk/for-organisations/data-protection-and-brexit/
3 ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
4 See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23297&LangID=E
5 www.edoeb.admin.ch/edoeb/en/home/documentation/annual-reports/26—taetigkeitsbericht-2018-20190/epaper-tb-26.html
6 UK Governments did not support the Data Surveillance Bill 1969, Personal Records (Computers) Bill 1969 or the Control of Personal Information Bill 1971.
7 For a good discussion, see Rosemary Jay, *Data Protection Law and Practice* (2012), p. 10.
8 See Letter of 16.12.2010 to Dr Chris Pounder from the European Commission: amberhawk.typepad.com/files/dp_infraction_reasons.pdf

Operational impact of the GDPR: Challenges for DPOs

How have DPOs and other privacy professionals coped with the first year of the GDPR in practice? Reported by **Robert Waixel** of Anglia Ruskin University.

This opening session of the *Privacy Laws & Business 32nd Annual International Conference* in Cambridge in July was a discussion between Lien Ceulemans, Vice President and Associate General Counsel – Global Privacy, Salesforce; Debbie Evans, Data Protection Professional and Lawyer, Kincordia; Olga Ganopolsky, General Counsel – Privacy and Data, Macquarie Group, Australia; and chaired by Garreth Cameron, Data Protection Officer, EMEA, Dentsu Aegis Network.

Ceulemans explained that Salesforce is a US based cloud computing company. Most of the risk in data processing involved the large amount of client data they hold. They need to be able to answer their client's privacy questions in a scalable way, regardless of jurisdiction.

Ganopolsky's company is an Australian investment bank. As such, privacy is the cornerstone in a more generalised risk management and highly regulated business environment with a worldwide reach, although it encompasses many different legal frameworks, and there is increasing convergence between privacy law, competition law and consumer law.

Evans currently works as Global Data Protection Officer for Rentokil Initial where she is responsible for implementing a data protection compliance policy program in over 70 countries. She had a legal and security background. She was concerned by the conflicting requirements of various laws worldwide.

What are the highlights of your GDPR implementation?

Evans said that buy-in was one of the big challenges for some areas. Although the need to prepare had been highlighted clearly beforehand, there were always some who woke up to GDPR challenges only as the implementation deadline loomed. Others realised that not everything could get fixed before the deadline and were more pragmatic. The uninitiated thought that buying an online tool and embedding it into the organisation would make the problem magically "go away". That was not the case.

The GDPR has been a generally positive experience for Ganopolsky, as it forms part of a broader legal program, which did not have an end date of 25 May 2018, since ongoing changes will still be needed. Other countries and states have legislation influenced by the GDPR and are enacting new laws that an organisation need to be compliant with, such as that in California.

Get a project manager

One key aspect that Ganopolsky highlighted is the need to have a professional Project Manager to help drive operational change. Lawyers and privacy professionals are not necessarily people with such skills.

Ceulemans added that she thought that leadership skills were also needed. Introducing GDPR compliance was a chance to see the privacy differences between jurisdictions, and influence change. Trust, understanding consumer's expectations and taking them seriously were at the heart of the matter particularly when talking to marketing departments.

Do you need top level buy-in?

Cameron posed the need for top-level buy-in. All the panel members agreed that buy-in is also needed on many other levels. Evans said: "It's a ripple effect. One needs top level buy-in, but all levels need their Privacy Champions. You get waves from the top and ripples from the bottom. Privacy Champions need a forum to discuss common issues, and the power to makes things happen."

How does a DPO field queries and get out the message?

Ganopolsky replied that especially in the Financial Services sector, one needs to lead from the top. It is important to recognise that people care about privacy in a new way. Some queries are comparatively new issues, such as data portability or new technology. Others are about basic individual rights such as consent. Whichever is the case, answers need to be tailored to the requester's needs, and presented differently depending on who is asking the question. She had invited a former High Court Judge and human rights advocate to speak on the OECD Privacy Guidelines at a conference she had organised, with colleagues believing that such a speaker would only attract a narrow and specialised audience. Against all expectations that session was a sell-out, showing the very high level of awareness and interest in the topic.

Cameron commented that it was important to keep going with waves of publicity to "keep getting the messages out". This was important not just in a burst when the GDPR was becoming live, but to keep continuing to maintain the audience's interest. Evans added that different strategies, forms and messages were needed depending whether communicating to professionals or specific groups. Comic strip messages may not be appropriate for every audience, some finding that format insulting, but alternatively a cartoon format might be a perfectly appropriate method for others. This can also vary between different parts of the organisation, geographical areas and cultures. Local Privacy Champions can be very helpful in this. Above all, "Keep it Simple" (or as simple as a complex topic can be) was a vital mantra.

Maintaining momentum

Communication was key with a high level of energy via Privacy Advocates

 © 2019 PRIVACY LAWS & BUSINESS

and whatever other means can be found. "The crisis is not over" said Evans, as there was the temptation to relax after the initial push to be 'ready' by GDPR-day. Organisations need to realise that the GDPR is a process for the long term and should be part of the 'business as usual' scene. Consumers are much more aware and are asking for more in terms of privacy, so it is an important way of gaining customer trust. Unfortunately, management can often just focus on GDPR fines – usually linked to data breaches. They need educating that GDPR compliance is a much wider concept. Failure is not just about fines, but also about having regulators taking a "detailed interest" in how you operate, which for most businesses is not a desirable outcome.

What structure do you use – DPO? CPO?

The panel was asked whether their firm had a DPO (Data Protection Officer) and/or Chief Privacy Officer (CPO) as part of their structure.

Evans said that in her case, they have a single Data Protection Officer (DPO) with local privacy officers as well in most of the 75 countries they operated in. Some jurisdictions required a local DPO appointee and that would be done if required.

As Ceulemans explained, the GDPR has influenced many laws worldwide, some being simplified from the EU version. Over the last two to three years there has been much interest worldwide, improved and more sophisticated internal and external educational conversations about privacy, and a continued developing respect for privacy.

In Australia, there is a right to data portability and privacy rights are also covered as part of consumers' legal rights. Tribunals have enforced a "Right of Fairness" which extended through privacy, employment and consumer laws.

Ganopolsky said that she also sees such convergence. It is a battle with legal complexities to try and present a harmonised approach despite the range of different data privacy laws. A common theme is the need to protect the rights of individuals and their personal data and to consult individuals, where practical, about the usage of personal data.

Can technology help?

All three panel members agreed that technology is helpful, and case management systems are useful particularly in a multinational context. Evans commented that when a new organisation has been acquired, integration is one of the biggest challenges, although things settle down eventually.

What would you do differently?

Ceulemans would have hired a professional Project Manager to run the GDPR transition programme. Evans said she would have liked to have written her own bespoke software for their in-house Data Protection Management system, as off the shelf systems do not always fit the way their business is run. Ganopolsky wished they had included in their GDPR roll-out some of the jurisdictions with less developed data privacy policies and not just the highly developed ones like California and Korea. When challenged, she admitted that this would have been a 'nice to have', but in practice difficult when faced with the immediate prioritisation of GDPR roll-out.

Benefits of interoperability in large systems?

For large systems, does interoperability make such systems more vulnerable to the threat from cyber attacks? Evans responded that some sensitive systems are designed not to be interoperable for exactly that reason, which mean that a central DPO needs to go to the owner of that system to get access to its data. There is a need to work very closely with the security team, in such areas and to label personal data very carefully, especially sensitive (now 'special category') data. Ceulemans talked about the need to reduce legacy systems where possible, and of course have a clearly policed and audited policy on access controls.

Is your organisation compliant with the GDPR?

The speakers thought that no organisation will actually ever be 100% compliant but should aim to be "as good as possible". Ceulemans, realistically, said: "You need to have a defensible position, but the bar is always being raised the further away from GDPR-day one gets."

AUTHOR

Robert Waixel is an Associate Lecturer at Anglia Ruskin University and as RW Systems an independent consultant, tutor and speaker. He has been part of the *PL&B* team of conference rapporteurs continuously since 1995.

ICO issues new cookie guidance

The Information Commissioner's Office states that implied consent is not acceptable under the GDPR – whether for cookies, or for processing personal data. Its new guidance, issued on 3 July, says that websites and apps must tell users clearly what cookies will be set and what they do – including any third party cookies. However, consent is not required for cookies that are defined as 'strictly necessary' – those that are essential to providing the service requested by the user, the ICO says.

On cookie walls, the ICO advises that using a blanket approach, a statement such as 'by continuing to use this website you are agreeing to cookies' is not valid consent. The ICO is interested in getting feedback on this point.

Cookie compliance will be an increasing regulatory priority, the ICO says. However, any future action would be proportionate and risk-based.

• *See ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/*

Data transfers: Unlocking the value of analytics in a 5G world

Big Data analytics would be made more efficient with global rules on data transfers, says **Barry Murphy** of Vodafone.

Data analysis already helps banks to provide the finance customers need, cities to manage traffic and telecommunications companies to improve their networks and services. Furthermore, we are on the precipice of 5G being widely available. This will drive substantial increase in various kinds of connected devices, in particular Internet of Things or IoT, and unlock new data insights. Cisco estimates that by 2022 there will be more than a billion wearable devices and mobile data traffic will increase to 930 exabytes (or three times all the data stored in the world by 2007[1]). In the UK, effective use of data can create £66 billion of new business and innovation opportunities, let alone the insights that could further help us in our daily lives. Yet international studies show that the vast majority of existing datasets are nowhere near fully used, with most companies surveyed estimating that they are analysing just 12% of their data[2]. Companies can only realise the value of their data to benefit both themselves and their customers by having access to the best technology and people around the world.

A key way of deriving value from data is by combining and analysing data to find aggregate, anonymous insights and trends, commonly called Big Data Analysis or Analytics. Data is aggregated into a large data set and an alphanumeric string is assigned to each unit of observation ("unit identifier"). Using a unit identifier is critical to modelling the behaviour of the same unit of observation across the various data sets. If the unit of observation connects to an individual (e.g. a device, an account-holder, a customer number), the unit identifier is pseudonymous which means that the data that is related to the same unit of observation can be matched without ever needing to identify the individual. Moreover, it is often not possible to use anonymous data to create insights as there would be no way to identify the same unit of observation across the various data sets and it would therefore be impossible to find patterns (e.g. it would be unclear whether it is the same user using a service one hundred times or one hundred users using the service once).

The global world of data analytics

Analytics is often performed across a global, digital eco-system. Companies will often rely on their own global service centres and third party companies to help them perform analytics: the equipment hosting the data may need a back-up in another location for disaster recovery; technicians servicing the equipment generally need to be located around the world in different time-zones to ensure continuity of service 24/7; and analysts and engineers needed for specialised technical processes (e.g. systems development) may not be located in the country where the data was originally collected or was subsequently stored. It is rare that all the components of the analytics life-cycle and value chain can be found in one place. Critical to the effectiveness of analytics, therefore, is making the data accessible to other people in other places.

Companies operating global analytics ecosystems will generally need to incorporate robust safeguards into their business processes to meet cross-border data transfer requirements. Some laws regulate the act of making people's data accessible to another person in another place (e.g. GDPR) and other laws require that data is localised within the borders where it was originally collected (e.g. Russia, Vietnam). Pseudonymous data necessary for analytics is regulated under many data protection regimes because it is sometimes possible to combine the unit identifier with other data to potentially identify an individual (i.e. it may be possible to identify an individual if you reconstitute the unit identifier back into their bank account number), although companies put technical and organisational controls in place to prevent reidentification. Whatever the cross-border requirements, companies face significant operational costs and administrative burdens in putting safeguards in place that satisfy the variety of data transfer rules that may apply to the processing necessary to perform analytics across a global eco-system, particularly if the processing is centralised in a global database.

Towards a global data transfer network?

Privacy professionals who have become adept at finding consensus across fragmented laws and complex digital eco-systems to permit the data transfers necessary for analytics will recognise that global rules on data transfers would be a significant step towards realising the value of global data. Indeed, Japanese Prime Minister Shinzo Abe has called on the G20 to find global consensus on data governance saying that "data drives everything" while acknowledging that personal data needs to be protected. Some actions taken by data protection authorities and companies demonstrate that finding global consensus on data transfers is possible and that collaboration between companies, governments and data protection authorities is critical to developing a global rules-based data transfer framework that unlocks the value of data.

Central to the success of any global data transfer framework will be the legal certainty it provides companies and the ease with which it can be used. One data transfer safeguard that has become a global standard among companies and other organisations are a set of contractual clauses adopted by the European Commission known as the Standard Contractual Clauses or SCCs. The SCCs oblige companies handling

 © 2019 PRIVACY LAWS & BUSINESS

people's data to comply with EU data protection law standards, grant individuals a right to compensation if their data is mishandled, and provide relevant regulators or third parties with audit rights over their processing facilities. Companies use SCCs to comply with GDPR regulatory requirements, contractual obligations or simply to demonstrate high data protection standards. Companies subject to GDPR prioritise using the SCCs to permit data transfers necessary for analytics due to the legal certainty that the SCCs provide in addition to the relative ease with which the SCCs can be incorporated into business processes compared to other GDPR data transfer mechanisms. Moreover, the use of SCCs where not required by law demonstrates companies' willingness to provide people with comprehensive privacy protections if the safeguard is easily incorporated into complex business processes and value chains.

A globally developed rules-based system must keep pace with technological change while always protecting individuals' privacy rights. In the SCCs developed in 2010, subcontracting is contingent on consent, whereas Art 28 GDPR which became effective in May 2018 says that the same subcontracting can occur with the "general written authorisation" of the company that controls the means and purposes of the data. The GDPR position better reflects the operational reality of performing analytics in such a complex value chain where obtaining consent from all companies in the digital ecosystem will not be possible. The change in law is an example of a movement towards principle-based rules that balance companies' operational needs with protection for individuals' privacy. This approach aligns with the principle-based requirements in legacy data protection laws that were so successful at keeping pace with the transformational technology changes during the nineties and noughties and should form the basis of a global rules-based data transfer framework.

Developing a global data transfer framework that requires significant investment or specialist expertise is unlikely to be sustainable or scalable across the entire analytics digital ecosystem. A data transfer framework that is widely adopted is key to protecting data subject rights. Comparing the subscription rate of two data transfer mechanisms gives us a sense of the scalability of different solutions. In the EU, one of the data transfer safeguards available to companies involves incorporating rules defined by an EEA authority into their company and receiving approval from a national EEA authority that they designate (referred to as Binding Corporate Rules or BCRs). BCRs involve a high level of interaction with data protection authorities to gain approval which usually takes 6-9 months and requires significant investment – 56 companies have registered for BCRs. In contrast, some US companies self-certify their privacy compliance under a scheme to permit data transfers between the US and the EEA called the Privacy Shield and 4000 companies use this scheme. In a recent survey, 88% of companies said that they prefer to use SCCs which as we have seen provide legal certainty and ease of use with very little investment. While there are fundamental differences in the data transfer mechanisms, there is a correlation between subscription rates and ease of use that should encourage the development of a data transfer framework that integrates to business processes.

Where are we now?

Globally, the decisions already taken by legislators data protection authorities and courts provide the knowledge necessary to overcome some of the operational challenges faced by companies implementing data transfer frameworks while enhancing privacy protections. Companies subject to GDPR have sought data protection authority approval for changes made to the prescriptive requirements in the SCCs (e.g. subcontracting and auditing rights). The changes to the SCCs that have been approved by data protection authorities provide good insight into the operational needs of many companies and they provide a framework for further global collaboration between data protection authorities, companies and other public interest groups to balance the need to realise the value of data with the overriding objective of always protecting people's privacy. Recent court challenges have also enhanced our understanding of privacy protections in fundamental and far-reaching ways – right to be forgotten, extra-territorial application of privacy protections, right to claim for distress, a data subject's right to claim in domestic courts, among others – which broadly have been codified into law by GDPR. Our knowledge and understanding of data transfer privacy protections will be further enhanced by the Court of Justice of the European Union (CJEU) decision in the Max Schrems challenge to the SCCs due later this year. The knowledge necessary to start developing solutions that balance the need to protect individuals' privacy with the benefits that analytics can bring to individuals on a global basis is available; it is a matter of businesses, Data Protection Authorities and legislators finding consensus.

Codes of conduct offer potential to address the challenges of complying with data transfer restrictions that apply to specific data processing activities, such as analytics. GDPR permits trade associations and other bodies to develop codes of conduct in collaboration with data protection authorities on specific GDPR issues, including data transfer safeguards. Many of the key components of a successful data transfer mechanism that we have touched on above are contained in a paper on codes of conduct adopted by the European Data Protection Board (EDPB) on 4 June 2019 (Guidelines 1/2019) – a practical framework that can keep pace with technological change, legal certainty, scalability, sustainability and ease of use. The EDPB has committed to publishing separate guidance in relation to the use of codes of conduct as a mechanism to facilitate data transfers at a later date. With current questions over the validity of SCCs as a consequence of Max Schrems' legal challenge – SCCs being the key data transfer mechanism for companies that must comply with GDPR – alternative mechanisms for data transfers such as codes of conduct cannot come soon enough. Moreover, analytics described in this article is a very precise form of data processing with generally tight, standardised controls surrounding identification of individuals that would lend itself to a global approach. A mechanism for mutual recognition of

the standards and codes across all global laws, whether in trade agreements or otherwise, may provide a template for balancing individual rights with the potential that analytics promises to provide.

Developing a principles-based global data transfer framework with comprehensive privacy protections would enhance the efficiency of performing analytics. Companies must articulate the need for a global data transfer framework for analytics in a way that allows data protection authorities to consider both the operational commercial benefits and the comprehensive privacy protections that companies have generally built into their analytics business processes (i.e. pseudonymisation and technical measures that prevent identification of individuals).

Globally, the decisions already taken by legislators and data protection authorities in relation to data transfers provide the knowledge necessary to start developing a global data transfer framework that integrates with a patchwork of data protection laws, and specifically for analytics in the digital age. Collaboration between companies and data protection authorities is key to developing a global data transfer framework that will unlock the value of analytics and transform people's lives – technology waits for nobody.

AUTHOR

Barry Murphy is Senior Privacy Counsel and Data Policy Advisor at Vodafone, London.
Email: barry.murphy4@vodafone.com

REFERENCES

1 www.bbc.co.uk/news/technology-12419672
2 www.gov.uk/government/publications/uk-digital-strategy/7-data-unlocking-the-power-of-data-in-the-uk-economy-and-improving-public-confidence-in-its-use#fn:4

What should administrators do when faced with Subject Access Requests?

The recent case of *Green v. Group Ltd and others* [2019] EWHC 954 (Ch) dealing with Cambridge Analytica's insolvency has clarified the approach that administrators should take when Subject Access Requests are made to the companies over which they are appointed, Reed Smith LLP reports.

During its investigation, the ICO had seized the companies' laptops and servers, which meant the business could not continue to trade. The failed attempts to market the business led the administrators to place the companies into compulsory liquidation and request that they be appointed as liquidators.

A creditor then complained that the administrators had breached duties arising under data protection laws. He sought an Enforcement Notice under the Data Protection Act 1998 against two group companies asking that they comply with a Subject Access Request to provide details of his personal data potentially held by the companies, Reed Smith lawyers Cynthia O'Donoghue and Curtis McCluskey say.

"The creditor also wrote to the administrators requesting copies of the materials and notes of the oral submissions made at the administration hearing. The administrators allowed the creditor's disclosure application, having rejected it initially, and eventually provided the requested documents."

"In its assessment of the creditor's objections, the High Court first referred to previous case law, which had established that a liquidator is not regarded as a controller in respect of personal data processed by the company. As a general rule, a liquidator acts as a company's agent and, unless the liquidator takes decisions about the processing of the data as a principal rather than an agent, the liquidator cannot be considered a controller."

"Here, the administrators decided not to search for the creditor's data through records of 700 terabytes which had been seized by the ICO. The court agreed that this was a decision that the administrators were suited to make. As agents of the company, the scope of their statutory duty was limited and the interests of one creditor had to be balanced against the interests of the general body of creditors. The court also said that administrators have no general duty to investigate data breaches by the company relating to third parties (such as data subjects). Their duty only extends to investigating breaches of the duty owed by the directors to the company or its creditors."

• *See www.lexology.com/library/detail.aspx?g=e654584f-9f77-4c0e-9b5b-d5968cfa71a3*

UK class action cases advance

SPG Law is representing consumers in the data breach case of British Airways. 185,000 of BA's customers were potentially affected last summer by a breach involving website and app customer data. SPG Law has since launched a group compensation (collective action) claim against the airline based on Article 82 of the GDPR.

The company says that BA's offer to reimburse customers who suffer "direct financial losses" and to offer "credit rate monitoring" is not good enough. It is pursuing a 'no win, no fee' claim and estimates that £1,250 is available for each claimant. "Whether or not regulators decide to fine BA, the company is one of the first to face the prospect of co-ordinated compensation claims since the GDPR took effect in the EU in May 2018," SPG Law says.

 © 2019 PRIVACY LAWS & BUSINESS

ICO in Northern Ireland: Business as usual?

The ICO has regional offices in Wales, Scotland and Northern Ireland. **Laura Linkomies** reports on developments in Northern Ireland.

Devolution means that we are dealing with three different legal systems in Northern Ireland, Scotland and Wales, Ken Macdonald, Head of ICO Regions explained at *PL&B's* conference in Dublin on 9 May. "In addition to legal differences, there are also some institutional ones. This is also reflected in regulatory action," Macdonald said. For example, in Northern Ireland, the ICO has two options:

1. Prosecute offences itself, or
2. Pass cases to the Police Service of Northern Ireland to conduct a prosecution.

They act independently and on their view of whether it would be in the public interest to proceed.

In Scotland, criminal prosecution is not included in the ICO's powers, as Scotland's judicial system is separate from that in England and Wales. The ICO reports suitable cases to the Procurator-Fiscal's (prosecutor's) office. These offices are staffed by legally qualified civil servants who receive reports about crimes from the ICO, the police and others and then decide what action to take in the public interest, including whether to prosecute someone.

The rationale for fining

Macdonald explained the rationale behind the ICO's fining policy. The Information Commissioner's public policy is that fines should be transparent, effective, proportionate, consistent and persuasive. They also undoubtedly help increase organisations' awareness of their legal obligations under the Data Protection Act. The risk to an organisation's reputation means that top management pays attention.

The fining process

Macdonald explained the process of setting fines at the ICO. Firstly, there is an initial assessment of the incident, the sequence of events followed by an analysis of the severity of the breach – number of people affected, number of records lost and the sensitivity of the data in question. The ICO will then look at any aggravating factors, for example could the breach have been avoided altogether? What action did the data controller take and when? Were the data controller's responses to the ICO's investigation "inaccurate and misleading?" The ICO is mindful of the deterrent effect of fines. A fine on a company in a particular sector may work well in raising awareness of bad business practices in the whole sector.

The ICO will also take into account mitigating factors – how well the organisation cooperates with the ICO, and whether it has a previous, clean track record. This include level of compliance where the ICO has previously demanded action, and what steps the organisation has taken to mitigate the incident. In some areas, adherence to codes of conduct or certification can work in the organisation's favour.

"No fines have yet been issued under the GDPR but we are getting close to issuing the first one in a few weeks' time," Macdonald said. However, Macdonald emphasised that for many companies, reputational damage is still more serious than any fine.

ICO in Northern Ireland

The ICO's six-person office in Belfast provides a local point of contact for members of the public and organisations based in Northern Ireland. It operates an advice service to address general enquiries on data protection and freedom of information. The staff promote good practice in information rights by raising awareness of organisational responsibilities across all sectors, the ICO says. It also influences policy in related areas by working closely with the departments of the Northern Ireland civil service and the wider public sector.

Impact of Brexit

How will Brexit affect data flows from Northern Ireland? Macdonald explained that data flows across the border to the Republic of Ireland, or any country outside of the UK will fall under the new UK transfer and documentation provisions. The UK is recognising that EEA countries will continue to have "adequate" data protection laws, as it hopes that, on leaving the EU, the European Commission will recognise that the UK's data protection law is also "adequate."

Data flows from the European Economic Area to Northern Ireland, as to any other part of the United Kingdom, require organisations to ensure that they have appropriate arrangements in place for a transfer to a third country, for example, Binding Corporate Rules, Standard Contractual Clauses or, in future, codes or conduct/certification mechanisms.

In some instances, organisations can rely on derogations where:

- an individual has expressly consented to the proposed transfer, having been provided with all necessary information about the risks associated with the transfer
- the transfer is necessary for the performance or the conclusion of a contract between the individual and the controller, or the contract is concluded in the interest of the individual
- the data transfer is necessary for important reasons of public interest
- the data transfer is necessary for the purpose of compelling legitimate interests of the organisation.

INFORMATION

ICO Northern Ireland contact details are:
The Information Commissioner's Office – Northern Ireland
3rd Floor, 14 Cromac Place,
Belfast BT7 2JB
Tel: 028 9027 8757 / 0303 123 1114
Email: ni@ico.org.uk

National data strategy: Making the best use of data for society

The government wants to "unlock the power of data in the UK economy and government, while building public confidence in its use." **Laura Linkomies** reports.

The government is developing a National Data Strategy to ensure that everyone can effectively participate in an increasingly data-driven digital society. Also, for the government itself, it is important that it can improve public services and government operations through the effective collection, sharing and use of data. How can these objectives be reached if individuals do not trust the way organisations process and share personal data?

The UK is keen to be at the forefront of these developments but is already lagging behind countries such as Estonia, where 99% of all public sector transactions are digital. All speakers at the Westminster e-Forum, held in London on 14 May, agreed that consumer trust is the key.

Roger Taylor, Chair of the Centre for Data Ethics and Innovation (the Centre), an advisory body set up by government and led by an independent board of expert members, said that the National Data Strategy is an opportunity to set some standards in this field. "One of the key functions of the centre is an advisory function. We need to identify best practice and distribute that. We must not be biased. But what is socially acceptable? The ICO is looking at this also."

"The Centre has been set to identify whether there are regulatory gaps. The ICO is focused on how far you can push the law to give people what they want. We look at complementary issues."

Simon McDougal, the ICO's Executive Director for Technology Policy and Innovation, said that cooperation with the Centre is a great example of constructive dialogue.

"Public trust is critical to national data strategy. Our information rights strategy aims at increasing public trust in how data is used. But it looks like we are not doing so well in the UK. We are having a crisis of trust. This is a challenge for regulators and anyone who advocates new and innovative uses of data. How did we get here? About ten years ago there were hugely ambitious government-driven data projects. As we all know, the majority of them stumbled – for example the ID card scheme. That eroded public trust, and, as a consequence, many large schemes were stopped. Then the private sector got involved and there have been spectacular issues in the last few years that have driven the crisis where we are now."

We need to find ways to engage with the public. People still use the data-driven services as it is convenient, McDougal said. He said that the ICO concentrates on three areas: Engage, enable, and enforce. The ICO's annual track survey shows that only 15 per cent of people have high trust in how organisations process their data. The ICO has now set up Citizens' Juries to discuss AI. "We have learned that when you explain these technologies, and the value of the service to the individual and society, it is a much more constructive discussion."

McDougal said that enabling the innovators and technologists to do it right the first time is part of the parcel. "Taking something as nebulous as ethics is not easy to apply. From principles to practice, that is the question."

Reflecting on the GDPR, he said: "The GDPR is more flexible than some people think. There are limitations, for example, on processing and societal harms but if talking about inferred data, the GDPR covers that. For example, insights about groups are based on individuals' data."

"But the GDPR legitimate interest test is tougher than people think. It is not a get out of jail card, but on the other hand GDPR is not just about consent."

Do we need regulation?

Mark O'Conor, Partner at DLA Piper, talked about the right level of the regulatory framework. "This is a time to reflect on law and ethics. Ethics was not central to lawyers' education, but is now at the forefront. We write contracts on monetising data analytics. Business needs to know what is right and what is expected, for survival and for a competitive edge. We need to unlock the power of data in the UK but as has been said, there is a low level of public trust."

Explainability is central to AI: how to get the public to see the advantages of AI? "We must make sure we do not take past prejudices forward into regulation. We have been working with a business school on the breakdown of trust, and there is a report coming out later this year. We looked at trust in terms of the fractured relationship between business and government. Now we are opening lines of communication; today's event is a good example of this."

"There is a commercial imperative for this work. Businesses, banks for example, need to explain why a customer has been declined a loan, for example. A common ethical framework is needed," O'Conor said.

In the US, there is $2 billion investment on examining explainability and common sense. Do we need to regulate? What is common sense? he asked.

Can we use AI to form a shortlist of job candidates? What is being done, what do people think you are doing and what are the implications of machine-made decisions? Transparency is key. Can we come up with an ethical framework? That is a tall order, but I think we can, O'Conor said. The legal framework is GDPR, Privacy by Design, DPIAs, and the ability to explain certain automated decisions. Do we need more law? I do not think so. But in certain cases, we need some restrictions, for example, for automated vehicles, now an issue for insurers, he said.

Jeni Tennison, CEO at the Open Data Institute, which is a not-for-profit

 © 2019 PRIVACY LAWS & BUSINESS

organisation, spoke about the challenges with using AI: people use services even if they do not trust the data processing and the sharing of their personal data. Is this the true feeling as opposed to survey results?

"Self-regulation is not enough. It is up to government to provide the enabling environment that creates trust. There is risk aversion to innovation. The use of data impacts us as a society. Legislation is needed for areas where we are already seeing a negative impact on democracy, for example, micro-targeting for political purposes. Data quality is also in danger - people start to give false answers when they do not trust data controllers."

Dr Brent Mittelstadt, Research Fellow at the Oxford Internet Institute, spoke about how to protect collective aspects of privacy. He said that consent is no longer useful when data can be repurposed. Consent should be a collective task rather than something that falls on an individual. Self-regulation seems to put the responsibility on companies to behave ethically, and problems are presented simply as technical issues that can be easily fixed.

"Do codes of conduct affect the behaviour of software engineers? I think not. It is very easy to sign up to a code when they do not require you to critically assess your business model. Are there any sanctions or enforcement mechanisms? If not, there is little value in codes."

Is there political will?

Daniel Zeichner MP, Chair of the all-party Parliamentary Group on Data Analytics asked whether there is political will. "These are difficult issues. There is a danger of inadvertently bringing about inequality. We follow things closely. The pace and scale of change has huge implications, and may be testing for our political structures. The responsibility should not be on the individual."

Patrick Stephenson, Client Managing Director at Fujitsu UK, spoke about the key requirements and priorities for the UK data infrastructure.

"Put citizens in control of their data. In Finland, it takes 18 seconds to process a tax return. This is result of data sharing between government departments. Estonia is thinking of legalising algorithms."

Algorithms are rapidly emerging as artificial persons: a legal entity that is not a human being but for certain purposes is legally considered to be a natural person. Intelligent algorithms will increasingly require formal training, testing, verification, certification, regulation, insurance, and status in law[1].

"This is in contrast with the UK. While some brilliant work has been done on digitalising, we have many legacy systems to deal with, and a large population." As there is complexity in accessing services, why not turn data inside out? "Let citizens manage their data. They will see for themselves that data is accurate, they will expect a digital government." According to Stephenson, key priorities would include citizen control, e-identity, a digital data vault - birth certificate etc, Right to be Forgotten, data portability and a pan-government data exchange platform.

Gaia Marcus, Head of the National Data Strategy at the Department for Digital Culture Media and Sport (DCMS) spoke about the next steps for the national data strategy.

"We aim to be collaborative and as open as possible. We have sector experts working with us from the public as well as from the private sector. We are in a listening mode. Public trust underpins the delivery of the national data strategy. We will be looking at unlocking the power of data. The notion of trust is troublesome, however. I think we need to talk about being trustworthy, and about transparency. We do not just look at personal data but the effect on the data economy."

What's next?

At EU-level, it has been said that the GDPR will inhibit the development and use of AI in Europe. The EU is therefore developing ethical guidelines for the use of AI to be in the lead in this area. In the UK, the DCMS has said that the Centre for Data Ethics and Innovation should be placed on a "statutory footing".

The DCMS recently launched a call for evidence for the National Data Strategy, which seeks views on the parameters and objectives of the strategy and aims to gather evidence that will underpin a draft strategy. The evidence-gathering session closes on 14 July 2019. The DCMS will run a full consultation on the draft strategy later in 2019.

The data protection issues identified by government include:

1. How can organisations demonstrate trustworthiness in their use of data?
2. How easy is it for the public to find out about how information provided to or inferred about them by an organisation is being used?
3. Are organisations using personal data in ways that may damage trust?
4. In what ways are companies making money from personal data? How profitable are these activities?
5. Do people know how information provided to, or inferred about them by an organisation is being used, stored and shared?
6. To what extent are people concerned about how data about them is used, stored and shared? Are some groups more concerned than others? Are there particular categories of data that raise more concerns than others?
7. What commercial practices or behaviours have affected trust in the use of personal data? Have targeted advertising and 'recommending' affected trust?
8. Have the GDPR and Data Protection Act 2018 made people more concerned about how personal data is managed? How has it influenced their behaviour?
9. How far do existing protections, such as those in the Data Protection Act, go in promoting transparency and trust? What, if anything, should the government do to further build trust?

INFORMATION

The Westminster e-Forum was held on 14 May, see www.westminsterforumprojects.co.uk
On DCMS evidence gathering, see www.gov.uk/government/publications/national-data-strategy-open-call-for-evidence/national-data-strategy-open-call-for-evidence

REFERENCE

1 www.legalfutures.co.uk/blog/algorithms-and-the-law

EU review of adequacy decisions well underway

The EU Commission's review of the existing adequacy decisions, which started two years ago, is due to be completed by May 2020 when the Commission will report to the EU Parliament and Council. Speaking at the *Privacy Laws & Business* 32nd Annual International Conference on 2 July, Bruno Gencarelli, Head of International Data Transfers and Protection Unit at the EU Commission, said that the Commission has asked the countries in question to update the Commission on any legislative changes and enforcement of their existing laws. The second series of questions from the Commission has addressed issues around access to personal data by law enforcement and national security agencies.

Gencarelli said that the Commission is looking for 'essential equivalence' as determined by the Court of Justice of the European Union, not an identical system to the GDPR. The aspects that are important include individual rights, and importantly, how the law is being enforced.

He said that the negotiations with Korea, which has applied for an adequacy decision, are at an advanced stage. One of the remaining issues, independence and enforcement powers of the DPA, is being addressed by an Amendment Bill which is pending in Korea's National Assembly.

There is no special order in which the Commission will review the existing adequacy decisions, or a queue of new applicant countries, Gencarelli said. Future candidates could include Brazil and Chile. When asked whether the Commission would suspend existing decisions due to an unsatisfactory review, Gencarelli said that he cannot rule out these types of measures but stressed that the Commission aims at continuity.

Negotiations with Japan, which now has a mutual adequacy decision with the EU, took two years, Gencarelli revealed. One of the trickiest aspects was onward transfers – an aspect that would also be a 'sensitive issue' in a possible UK adequacy application.

ICO report: GDPR one year on

The ICO says in its Report - GDPR: One Year On – that it received 14,000 personal data breach reports from 25 May 2018 to 1 May 2019. For comparison, it received around 3,300 reports in the year from 1 April 2017.

EU Data Protection Board figures indicated that from 25 May 2018 to 1 May 2019, there were around 240,000 cases across the EU (data protection complaints, data breaches, proactive investigations or other similar issues). The ICO received over 55,000 of these (roughly 23%). Where the data protection cases reported have cross-border implications throughout the EU, these are reported to a lead EU Data Protection Authority. The UK is currently the lead supervisory authority on 93 of these cases.

In addition, the UK is working on behalf of UK citizens to uphold their information rights in 58 other cases where other EU Data Protection Authorities are the lead supervisory authority, and the UK is a concerned supervisory authority.

The ICO says that most Data Protection Officers (DPOs) seem to be well-positioned. When it surveyed DPOs this spring, the responses showed that the majority of DPOs felt that they received great support from within their organisation. The importance of culture was considered to be one of the biggest issues for implementing the GDPR. Around two-thirds of all respondents were satisfied with their senior leadership support. More than 90% of DPOs had an accountability framework in place and 61% reported that their framework is well understood in their organisation. Overall, three-quarters of DPOs said that their information rights messages were getting through to their senior leadership team, and they felt supported in developing a framework to embed these rights in their organisation.

• *See ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/05/gdpr-one-year-on/*

Study considers privacy and crisis management

Trilateral Research is currently looking at the key challenges in crisis management technology, and how the emerging privacy issues can be better tackled by adopting an ethical approach.

"Crises and disasters are increasingly understood to be complex events that require data from across borders and disciplinary understandings to build complete and actionable situational awareness. To support the multifaceted data needs to build situational awareness, information technology (IT) are often sought as solutions. These solutions are often based in machine learning and data analytics to help filter and gain useful insights from the big, diverse, and inconsistent data gathered through these systems," Trilateral says.

The aim of the study is to identify how to avoid misrepresentations, unintentional bias, function creep, increased fragmentation, and new forms of liabilities and power struggles for those using the IT.

The researchers are working with planners and technology designers to develop both IT and organisational tools to help address these ethical implications.

• *IN-PREP is an EU funded project made up of 20 partners representing seven EU Member States. See trilateralresearch.co.uk/using-data-to-enhance-collaborative-crisis-management/*

 © 2019 PRIVACY LAWS & BUSINESS

White Paper on online harms threatens freedom of expression says NGO

Index for Censorship, a Non-Governmental Organisation, states that the government's proposals for regulating online harms would hamper freedom of expression. The proposals include a statutory "duty of care" on companies that "allow users to share or discover user-generated content or interact with each other online". Facebook and Twitter would be covered, but also search engines, messaging services, and online forums. This obligation needs to be limited and defined in a way that addresses the risk that it will create a strong incentive for companies and others to censor legal content, the organisation says.

The NGO stresses that Parliament must be fully involved in shaping the government's proposals for online regulation as the proposals have the potential to cause large-scale impacts on freedom of expression and other rights.

"It is important to widen the focus from harms and what individual users do online to the structural and systemic issues in the architecture of the online world. For example, much greater transparency is needed about how algorithms influence what a user sees."

Index on Censorship has filed an official alert with the Council of Europe over threats to media freedom in the White Paper. The government's consultation closed on 1 July.

• *See www.indexoncensorship.org/2019/06/the-uk-governments-online-harms-white-paper-implications-for-freedom-of-expression/ and www.gov.uk/government/consultations/online-harms-white-paper*

Government eyes crime-busting data analytics

The government aims at more efficient government transactions and data sharing to reduce crime. Challenges on the way include the absence of a unique person identifier and maintaining accurate data in a population where circumstances change often (employment status, relationship status etc). One of the biggest challenges around AI is that it is only as good as the data used to train it. Poor data results in poor AI engines, the government says in its paper: *Tackling Fraud in Government with Data Analytics*.

The information sharing provisions stem from Part 5 of the Digital Economy Act 2017 (DEA). Public sector access to data has been hindered by a complex legal framework that has grown piecemeal over time, the government says. "Public authorities have found it increasingly difficult to understand what information they can share. The powers within Part 5 of the DEA are designed to help overcome these legislative barriers. The codes of practice associated with the information sharing provisions set out how the powers must be operated. The data sharing powers arising from the DEA must be exercised in compliance with the Data Protection Act 2018 thereby ensuring data is handled securely."

• *See www.gov.uk/government/publications/tackling-fraud-in-government-with-data-analytics and the National Audit Office paper on using data across public services: www.nao.org.uk/report/challenges-in-using-data-across-government/*

Environmental Information Regulations decision on costs

When calculating charges on responding to requests under the Environmental Information Regulations 2004 (EIR), organisations could consider whether they fall under the "appropriate limit" provided by the FOIA. The ICO's decision notice of 3 June on Folkestone and Hythe District Council however, says that the fee of £325 proposed by the Council was excessive.

The requestor was seeking the agendas, circulated documents, and minutes relating to meetings held by the Kent Planning Officer's Group (KPOG). The Council had explained that this is an informal forum for senior and head planning officers of the various local authorities based in Kent, including Kent County Council and Medway Unitary Council. KPOG is not a decision-making body, and functions only as a platform for sharing best practice and working initiatives between planning officers.

The Council had informed the ICO that it had a charging policy for the EIR. This policy contained the provision to charge a rate of £25.00 per hour for officer time spent complying with a request (not including time required for redaction under exceptions) in addition to the material cost of disbursements.

While the charge of £25 an hour would be reasonable under FOIA (the appropriate limit is £450 for local public authorities), the Commissioner thought that the charge of £325 is likely to "represent a significant cost to a requester under the EIR, and in particular, notes that the request seeks information about planning across the county; which suggests that the information may have a wider public value beyond the complainant's own immediate interest".

• *See ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/blog-counting-the-cost-of-accessing-environmental-information/*

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
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

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, formerly Data Privacy & InfoSec Officer, John Lewis Partnership

Subscription Fees

Single User Access

UK Edition **£450 + VAT***
International Edition **£560 + VAT***
UK & International Combined Edition **£900 + VAT***
* VAT only applies to UK based subscribers

Multi User Access

Discounts for Multiple User licence (up to 10) and Enterprise licence (unlimited users).

Subscription Discounts

Introductory discount (first year): 30% off for DPAs, public sector, charities, academic institutions, use code SUB30; 20% off for other organisations, use code SUB20.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £25, Outside Europe = £35

Combined International and UK Editions
Rest of Europe = £50, Outside Europe = £70

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