ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

UK seeks an independent data protection policy

Full alignment with the GDPR cannot be taken for granted any longer as Boris Johnson, the Prime Minister, steers away from commitments made in the Withdrawal Agreement. By **Laura Linkomies**.

The UK's negotiating mandate with the EU on the UK-EU future relationship, published on 27 February, states that the "UK will have an independent policy on data protection at the end of the transition period and will remain committed to high data protection standards". This strategy is set and the focus is now on making it work.

The UK is seeking two adequacy decisions from the EU (one under

Continued on p.3

ICO publishes final online Age Appropriate Design Code

DPIAs, high level privacy settings and switching profiling "off" by default are aspects required by this code, subject to Parliamentary approval. By **Ben Slinn** of Baker & McKenzie.

On 21 January 2020 the ICO published its Age Appropriate Design Code of practice for online services following a public consultation in April 2019[1]. The ICO is required to prepare this statutory Code under Section 123 of the Data Protection Act 2018. In terms of next steps, the Code needs to be approved by Parliament, and following such approval there will be a 12-month transition period before

Continued on p.4

Issue 108 **MARCH 2020**

UNITED KINGDOM
report

ISSUE NO 108 **MARCH 2020**

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

Ben Slinn
Baker & McKenzie

Victoria Hordern
Bates Wells

Marta Dunphy-Moriel and Alexander Dittel
Kemp Little

Abigail Dubiniecki
Strategic Compliance Consulting

Claire Robson
Great Ormond Street Hospital Children's Charity

Emma Erskine-Fox and Gareth Oldale
TLT

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

comment

Negotiations on EU-UK future relationship start in Brussels

The first round of the EU-UK future partnership negotiations have started, and will be followed by further negotiation rounds every two to three weeks in Brussels and in London. A high-level meeting is planned for June 2020. For data protection, if negotiations on adequacy for data transfers from the EU to the UK are simply at a technical level, the proposed timescale (end of 2020) could just be workable. However, at a political level, if data protection is used as a bargaining chip in the negotiations, things get much more complicated.

In the meantime, the UK is starting to conduct its own adequacy assessments (see p.1). It is hoped that the UK adequacy assessments and decisions can be taken more quickly than the EU has done, but this remains to be seen. For now, everything remains business as usual as the GDPR will continue to apply in the UK, and UK and EEA-based controllers will not need to take any immediate action. But as the Prime Minister seems to be more than willing to steer away from the GDPR, we need to monitor developments closely and, no doubt, organisations are paying even more attention to alternative transfer mechanisms.

In this issue we assess developments in biometrics (p.19 and p.22), and the emerging Children's Code which still needs Parliamentary approval but will signify a shift in attitudes and practice (p.1). A different kind of dilemma is the interface between anti-money laundering and data protection laws. Can there ever be common ground? Perhaps, suggests our correspondent on p.14.

The ICO is considering its role in the data ethics debate with a view to launching a public consultation in the second quarter of 2020. Read my interview with Ellis Parry, who is the ICO's newly appointed Data Ethics Adviser, Technology and Innovation. The ICO is again expanding its horizons to new areas (p.7).

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.

Age ... from p.1

the Code takes effect. The ICO expects the transition period to end in autumn 2021.

The Code is likely to have a significant impact on the design of online services and related data protection compliance. The ICO launched a consultation on 26 February 2020 (open until 27 March 2020) on a package of support it intends to publish to assist organisations with conforming to the Code[2].

The Code sets out a bold new vision for how online services likely to be accessed by children under the age of 18 should be designed from a data protection perspective, as well as aiming to instigate significant change not just in the UK. The Information Commissioner notes in her foreword that the Code is "the first of its kind" and is intended to "lead to changes in practices that other countries are considering too".

What does the Code apply to?

The Code can apply to more services that you may initially expect. The Code applies to "information society services" which are "likely" to be accessed by children. Children, for these purposes, is anyone under the age of 18, which follows the approach set out in the United Nations Convention on the Rights of the Child.

The Code applies to new as well as existing services. Therefore, existing services should be reviewed to determine if they are within the scope of the Code and if so, assess what steps are required to comply with the Code.

It is not the case that all services that children could possibly or theoretically access are subject to the Code, and factors taken into account in determining whether the Code applies would include the nature and content of the service, whether it has particular appeal for children, the way the service is accessed and any measures that are in place to prevent children from accessing the service.

However, if an online service is "likely" to be accessed by a child, then the Code will apply. This is determined on the basis of whether it is more probable than not that children will access or use the service. Therefore, the Code has a much wider reach than just services that are specifically aimed at children.

In practice this means many online services may be subject to the Code, including apps, programs, connected toys and devices (including "home hub" interactive speakers), search engines, social media platforms, streaming services, online games, news or educational websites and websites that offer goods or services over the Internet.

The Code does not apply to certain online services including some provided by public authorities (if not typically provided on a commercial basis), websites which just provide information about a real world service or

business, traditional voice telephony services (although Internet based voice/VOIP is within scope), preventative or counselling services as well as general broadcast services (although on demand services are within scope).

What does the Code actually require?

The Code includes 15 standards of age appropriate design for services that it applies to. This has been reduced from the consultation version which included an additional standard regarding governance and accountability, although governance and accountability are still addressed in the Code.

Best Interests of the Child: The best interests of the child is the primary consideration when designing/developing an online service likely to be accessed by a child, which requires considering the needs of the child and deciding how these needs can be best supported in the design of the service. It is possible to pursue your own commercial or other interests, but if there is a conflict, the ICO's view is that commercial interests are unlikely to outweigh a child's right to privacy.

Data Protection Impact Assessments: A DPIA will be required for online services likely to be accessed by children. Such DPIAs will need to include additional elements in each stage of the DPIA to assess, explain and document how each of the standards of the Code have been complied with. In addition, the ICO's expectation is that larger organisations should conduct some form of consultation with children and parents in most cases as part of the DPIA process.

Age Appropriate Application: One of the main changes to the standards from the consultation version is that Age Appropriate Application now requires a "risk-based approach" to recognising the age of users to effectively apply the standards of the Code to children. In addition, rather than applying the standards of the Code to all users unless there is a "robust" age verification mechanism in place to distinguish between adults and children, the final version of the Code states that either the age of the user should be established with a "level of certainty" that is appropriate to the risks to the rights and freedoms of children from the data processing, or the standards of the Code should be applied to all users. The protections and safeguards in place should be tailored to the age of the child.

Transparency: The privacy information provided to children should be prominent, concise and in clear language that is appropriate to the age of the child. This can include "bite-sized" explanations at the point that personal data is collected, as well child-friendly presentation including diagrams, cartoons, graphics, video/audio, gamified or interactive content. The ICO's expectation is that if user testing is not conducted, organisations should document the reason why in the DPIA.

Detrimental use of data: This standard is potentially very wide, and requires that children's personal data should not be used in a way that has been shown to be detrimental to their wellbeing, or goes against industry codes of practice, government advice or other regulatory provisions. The Code advocates a pre-cautionary approach, so even if there is no definitive evidence of detriment to wellbeing (e.g. if further research or evidence is required to determine this) then children's personal data should not be used for that purpose.

Policies and Community Standards: The ICO's general principle here is say what you do, and do what you say. The ICO expects you to uphold your own published terms, policies and community standards (e.g. privacy policies, age restrictions, content policies and behaviour rules/community guidelines).

Default Settings: Default settings should be "high privacy", unless you can demonstrate a compelling reason for a different default setting, taking into account the best interests of the child. Children should not be "nudged" towards selecting a lower privacy setting. Privacy settings should be provided for any processing of children's personal data for additional or optional elements of the service that go beyond the core service (e.g. personalisation).

Data Minimisation: Only the minimum amount of personal data should be collected and retained to provide the element(s) of the service that the child is actively and knowingly engaged in, and children should be given separate choices over which elements they wish to activate.

Data Sharing: Children's personal data (including inferred or derived data) should not be disclosed unless you can demonstrate a compelling reason for doing so, taking into account the best interests of the child. In the ICO's view it is unlikely that selling children's personal data for commercial re-use would be a compelling reason.

Geolocation: Options for collecting geolocation data should be turned off by default, unless you can demonstrate a compelling reason for having geolocation on by default, taking into account the best interest of the child. In the ICO's view any geolocation services that are additional to the core service should be subject to a separate privacy setting. When location tracking is active, an obvious sign should be provided to the child. Options that make a child's location visible to others must revert to "off" by default at the end of each session.

Parental Controls: Age appropriate information must be provided to children about parental controls if these are provided as part of the service. An obvious sign must be provided to children when they are being monitored if the service allows the parent or carer to monitor the child's behaviour online or track their location.

Profiling: Options which use profiling should be switched "off" by default, unless you can demonstrate a compelling reason for profiling to be on by default, taking into account the best interests of the child. Most profiling should be subject to a privacy setting, and only profiling that is essential to the core service (completely intrinsic to the service) would not require such a setting. In the ICO's view, privacy settings should always be provided for behavioural advertising used to fund the service, where it is not part of the core service the child wants to access. In addition, profiling should only occur if there are appropriate measures in place to protect the child from any harmful effects (in particular content that is detrimental to health or wellbeing).

Nudge Techniques: Nudge techniques (features that encourage or lead users to follow a preferred path) should not be used to encourage

children to provide unnecessary personal data or weaken or turn off their privacy protections.

Connected Toys and Devices: Connected toys or devices must include effective tools to enable compliance with the Code. By default, such services should be suitable for use by children, and user profile options for regular users could be implemented to support use by adults or tailor the service to the age of the particular child. This applies to devices obviously intended for children such as connected toys, but is much wider and applies to any connected device likely to be used by multiple users of different ages including children, e.g. "home hub" interactive speakers.

Online Tools: Prominent and accessible tools tailored to the age of the child should be provided to help children exercise their data protection rights and report concerns.

What should we start doing to prepare?

Although the Code is not likely to take effect until autumn 2021, organisations should start to prepare now in terms of changing design processes and reviewing existing services to ensure they conform to the standards of the Code.

The first step is to work out whether the Code applies to your existing services. Since the Code can potentially apply to a much wider range of services that just those traditionally viewed as being targeted at children, you should take particular care when carrying out this assessment. If you reach the conclusion that the Code does not apply, the ICO expects you to have documented the reasons why.

If you conclude that the Code does apply to your service, you will need to be prepared to demonstrate to the ICO how your services comply with the standards of the Code. A good way of doing this would be to document how you have complied in practice with each of the requirements of the Code (for example via an updated DPIA), and be in a position to be able to provide the ICO with copies of relevant policies, DPIAs, training and records of processing if required.

In practice, in order to prepare you will need to consider:

- updating DPIA templates to include additional areas demonstrating how the service complies with the standards of the Code, as well as conducting/updating DPIA on existing services and consulting with children/parents where necessary;
- reviewing existing/introducing new age verification mechanisms where necessary;
- reviewing/creating new information and resources for child users appropriate for their age, and testing this where appropriate;
- ensuring age appropriate tools are in place for children to exercise their rights under data protection laws;
- reviewing your existing services and ensuring design changes are made where necessary in light of the standards set out in the Code, including default privacy settings, profiling, nudge techniques, just in time notices etc.

What happens if we do not comply?

The ICO is required under the Data Protection Act 2018 to take compliance with the Code into account when deciding if an online service has complied with the GDPR and Privacy and Electronic Communications Regulations 2003 (PECR).

Regulatory enforcement action is a realistic possibility given that children's data is one of the ICO's regulatory priorities. The ICO has stated that where it seems that harm or potential harm to children is likely, it will take more severe action against a company than it otherwise would for other types of personal data. The ICO has also stated it is more likely to take formal enforcement action if proper steps have not been taken to comply with the Code and there is clear evidence or constructive knowledge that children are likely to access the service, and clear evidence of a significant risk from the use of children's data.

Complying with the standards of the Code will be a key way of demonstrating compliance with data protection laws in the context of online services likely to be accessed or used by children.

AUTHOR

Ben Slinn is a Senior Associate at Baker & McKenzie LLP.
Email: Benjamin.Slinn@bakermckenzie.com

REFERENCES

1 ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/information-commissioner-s-foreword/
2 ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/02/ico-consultation-on-a-package-of-support-for-the-providers-of-online-services/

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, 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 privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
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.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access UK events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. 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.

privacylaws.com/reports

"*PL&B* reports are one of the best sources of data protection information available today, especially the articles written by experienced practitioners who generously share insights and knowledge. In terms of quality, *PL&B* reports are in a league of their own."

Lucy Inger, Director, Lawmatrix

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 33rd year. Comprehensive global news, currently on 165+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

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