Volume 14, Issue 12
cecileparkmedia.com

DATA PROTECTION LEADER

A **Cecile Park Media** publication | December 2017

New year, new UK Data Protection Act

Ruth Boardman and Emma Drake of Bird & Bird LLP provide a summary of the UK Data Protection Bill 2017 and highlight some of the areas of uncertainty and debate, setting out what comes next.

CPM CECILE PARK MEDIA

CECILE PARK MEDIA

Editor Eduardo Ustaran
eduardo.ustaran@hoganlovells.com

Managing Editor Alexis Kateifides
alexis.kateifides@dataguidance.com

Editorial Assistants
Rachael Nelson-Daley, Cristina Ulessi, Kaveh Lahooti, Hernán Romero-Dutschmann, Ellen O'Brien

Data Protection Leader is published monthly by Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND

Telephone +44 (0)20 7012 1380

Website cecileparkmedia.com

Eduardo Ustaran Partner
eduardo.ustaran@hoganlovells.com
Hogan Lovells International LLP, London

Editorial: Seeking GDPR guidance from regulators? Be careful what you wish for

Everyone wants guidance. Everyone is asking for guidance. As the deadline for the application of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') approaches, everyone is clamouring for guidance. And the Article 29 Working Party ('WP29') has indeed delivered.

Emboldened by the forthcoming EU data protection framework, the regulators have invested considerable time and effort to consolidate their individual positions and provide clarity about their thinking. The result is a number of guidelines - some in their final version and some in draft - that have become crucial points of reference for those seeking to comply with the ever so complex GDPR. Yet, many of the points of view expressed in these guidelines have raised some eyebrows. By way of example, here are some of the most controversial interpretations of the GDPR featured in the various sets of guidelines issued by the prolific WP29 during 2017:

"WP29 considers that the right to data portability covers data provided knowingly and actively by the data subject as well as the personal data generated by his or her activity. This new right cannot be undermined and limited to the personal information directly communicated by the data subject." (WP 242, April 2017)

So this right is meant to apply not only to personal data actively and knowingly provided by individuals, but also to items such search history, traffic data, location data or raw data generated by the mere use of an app.

"'Core activities' can be considered as the key operations to achieve the controller's or processor's objectives. These also include all activities where the processing of data forms as inextricable part of the controller's or processor's activity. For example, processing health data, such as patient's health records, should be considered as one of any hospital's core activities and hospitals must therefore designate data protection officers." (WP 242, April 2017)

This has the potential for extending quite considerably the cases where regulators would expect organisations to appoint a data protection officer as required by the GDPR.

"The burden of proof ultimately falls on controllers and processors to demonstrate to the relevant supervisory authorities where the relevant processing decisions are taken and where there is the power to implement such decisions. Effective records of data processing activity would help both organisations and supervisory authorities to determine the lead authority. The lead supervisory authority, or concerned authorities, can rebut the controller's analysis based on an objective examination of the relevant facts, requesting further information where required." (WP 244, April 2017)

In practice, this sets a very high bar for the selection of a suitable lead supervisory authority which requires methodically documenting how and where decisions about data activities are made.

"As a matter of good practice, a Data Protection Impact Assessment ('DPO') should be continuously reviewed and regularly re-assessed. Therefore, even if a DPIA is not required on 25 May 2018, it will be necessary, at the appropriate time, for the controller to conduct such a DPIA as part of its general accountability obligations." (WP 248, October 2017)

This stresses the ongoing nature of the obligation to carry out DPIAs – something that organisations may not have immediately considered.

"As a rule, there is a prohibition on fully automated individual decision-making, including profiling that has a legal or similarly significant effect." (WP 251, October 2017)

According to this simple statement, if the data processing behind, say, online advertising activities strays into the realm of making decisions that significantly affect individuals, this processing is, by default, prohibited. It will then be for those involved in online advertising activities to obtain explicit consent in order to lawfully use the data.

"When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose." (WP 259, November 2017)

As a final example of how high the data protection authorities see the bar set by the GDPR, this would lead to a multiplicity of opt-in boxes whenever consent is selected as the lawful ground for processing. Of course, the regulators are not tasked with writing the law but with interpreting and enforcing it. Their guidance is certainly useful in that it accurately reveals their expectations. But it also highlights like nothing else, how challenging getting everything right by 25 May 2018 is going to be.

Ruth Boardman Partner
ruth.boardman@twobirds.com
Emma Drake Associate
emma.drake@twobirds.com
Bird & Bird LLP, London

New year, new UK Data Protection Act

By the time this issue of *Data Protection Leader* is in print, the Data Protection Bill 2017 ('the Bill') will have nearly finished its passage through the House of Lords. It seems likely that it will receive Royal Assent sometime in April 2018. Ruth Boardman and Emma Drake, Partner and Associate at Bird & Bird LLP respectively, provide a summary of the Bill (useful for those put off by its 203-page length and complexity), highlight some of the areas of uncertainty and debate, and set out what comes next.

The Bill is significantly more complicated than the Data Protection Act 1998 ('the 1998 Act'). It has seven Parts and 18 Schedules. A few moments consideration, however, is enough to realise that this increased complexity is inevitable.

When the UK implemented the Data Protection Directive (95/46/EC) ('the Directive'), it took a policy decision to extend the provisions of the Directive into areas outside EU competence. The result was the 1998 Act, setting out common rules for all personal data processing in the UK, albeit with specific exemptions for areas such as law enforcement and national security. This one-size-fits-all approach is no longer possible.

The structure of the Bill

As of 25 May 2018, the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') will automatically apply to all areas within EU competence. This necessitates the repeal of the 1998 Act and the adoption of new legislation to address the areas where the GDPR either requires Member States to legislate (for example, mandatory provisions relating to the constitution and powers of the supervisory authority for data protection, the Information Commissioner's Office ('ICO')) or permits Member States to legislate (for example, introducing additional circumstances when special categories of data may be processed, or introducing additional derogations from individual rights). In almost all cases, these are areas where the Directive also allowed Member States to introduce derogations or supplemental provisions. The approach of the Government has been to seek to carry forward the equivalent provisions in the 1998 Act or in the secondary legislation made under it. As stated in the Explanatory Notes, 'The Bill makes use of derogations where it is possible to achieve further consistency [with the 1998 Act].' As a result, although the layout of the Bill is different to the 1998 Act, much of the actual content will be familiar to practitioners.

In parallel, by 5 May 2018, the UK must have implemented the Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680) ('the Law Enforcement Directive'). This requires a similar, but not identical, regime to the GDPR to be put in place. As this is a directive, not a regulation, it requires the UK to legislate for the data protection principles, in a way which is not necessary (or indeed permitted) for the GDPR. This necessitates two separate sets of rules in the Bill.

The UK cannot stop at legislation that addresses the GDPR and the Law Enforcement Directive, however. As the 1998 Act will be repealed, this would leave certain areas - national security and other areas outside EU competence (for example, laws relating to education, defence and consular services) - without any data protection laws in place. Quite aside from its current EU commitments, the UK is a signatory to the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ('Convention 108'). Repeal of the 1998 Act, without putting in place replacement legislation in these areas, would, therefore, put the UK in breach of its commitments under Convention 108. The Bill will address this gap. As the new EU law already requires the UK Government to make a distinction between personal data processing for law enforcement purposes and for other purposes, it is probably no surprise that the Government has chosen to follow this pattern, and to have separate provisions for national security and other areas.

This leaves the UK with the four parallel sets of rules found in the Bill. When reading the Bill, it can therefore be helpful to have the summary below to hand:

Part 1: Preliminary

Introductory provisions and definitions of key terms (there is also a full index of defined terms later).

Part 2: General processing

GDPR related provisions

For example, these address:

- which persons will count as 'public authorities' or 'public bodies' for GDPR purposes (broadly, public authorities for Freedom of Information Act 2000 purposes);
- the age below which parental consent will be required for information society services where the lawful basis for processing is consent (13) (although this has been the subject of significant debate in the House of Lords).

Associated schedules:

Schedule 1: Special category data rules

This sets out additional conditions when special categories of data (in UK terms, sensitive data) and criminal conviction data can be processed. These build on the conditions in

1. https://hansard.parliament.uk/Lords/2017-10-30/debates/742E113F-2770-49B4-9985-47300C8268A4/DataProtectionBill(HL)
2. M. Moore, "Lib Dem peers 'hijack' Data Protection Bill to push for press watchdog", The Times, 2 November 2017.

Schedule 3 of the 1998 Act and associated secondary legislation. Some conditions are new (for example, more extensive conditions relating to processing of personal data for insurance and occupational pension schemes and new provisions allowing processing of data to prevent doping in sport).

There are also new requirements for those wishing to rely on these special conditions, who must have appropriate safeguards in place, via policy documents (particularly addressing retention and erasure) and supplements to the usual record of processing activities.

Schedule 2: Exemptions from the GDPR
As with the rules on special categories of data, many of these will be familiar from the 1998 Act. As with all elements of the Bill, there is a more complex structure:

Part 1: derogations from individuals' rights, fair processing and purpose limitation: similar to the 1998 Act's derogations for prevention & detection of crime and for processing in connection with legal proceedings, as well as a new condition relating to immigration control.

Part 2: derogations from individuals' rights: for example, covering derogations in the 1998 Act dealing with functions designed to protect the public.

Part 3: rules on third party data (i.e. the need to balance the interests of different data subjects when dealing with access requests).

Part 4: restrictions to data subject information and access rights: all broadly equivalent to current derogations in the 1998 Act (for example, the derogations for management forecasts and confidential references).

Part 5: freedom of expression and information.

Part 6: rules for research, statistics and archiving (i.e. addressing Article 89 of the GDPR).

Schedule 3:
This collates the current special provisions for health, social work, education and child abuse (currently set out in multiple statutory instruments) in one place.

Schedule 4:
Re-legislates the current derogations relating to laws that restrict access rights (for example, addressing adoption and human fertilisation and embryology considerations).

Schedule 5:
Provisions for accreditation of certification providers.

'Applied GDPR' provisions
In order to address the gap left by the repeal of the 1998 Act, the Bill chooses to 'apply' the GDPR by reference. Clause 20 of the Bill provides that 'the GDPR applies to the processing of personal data to which this chapter applies but as if its articles were part of an act extending to England and Wales, Scotland and Northern Ireland.'

Associated schedules:
Schedule 6:
The GDPR cannot simply apply as is to areas outside European Commission competence. By way of example, the rules in the GDPR requiring processing with cross-border impact to be subject to the consistency mechanism, or providing for the role of the European Data Protection Board can have no application.

Schedule 6 lists out the detailed modifications to the GDPR for the applied GDPR to work. It may, therefore, also serve as a good indicator of UK data protection law post-Brexit.

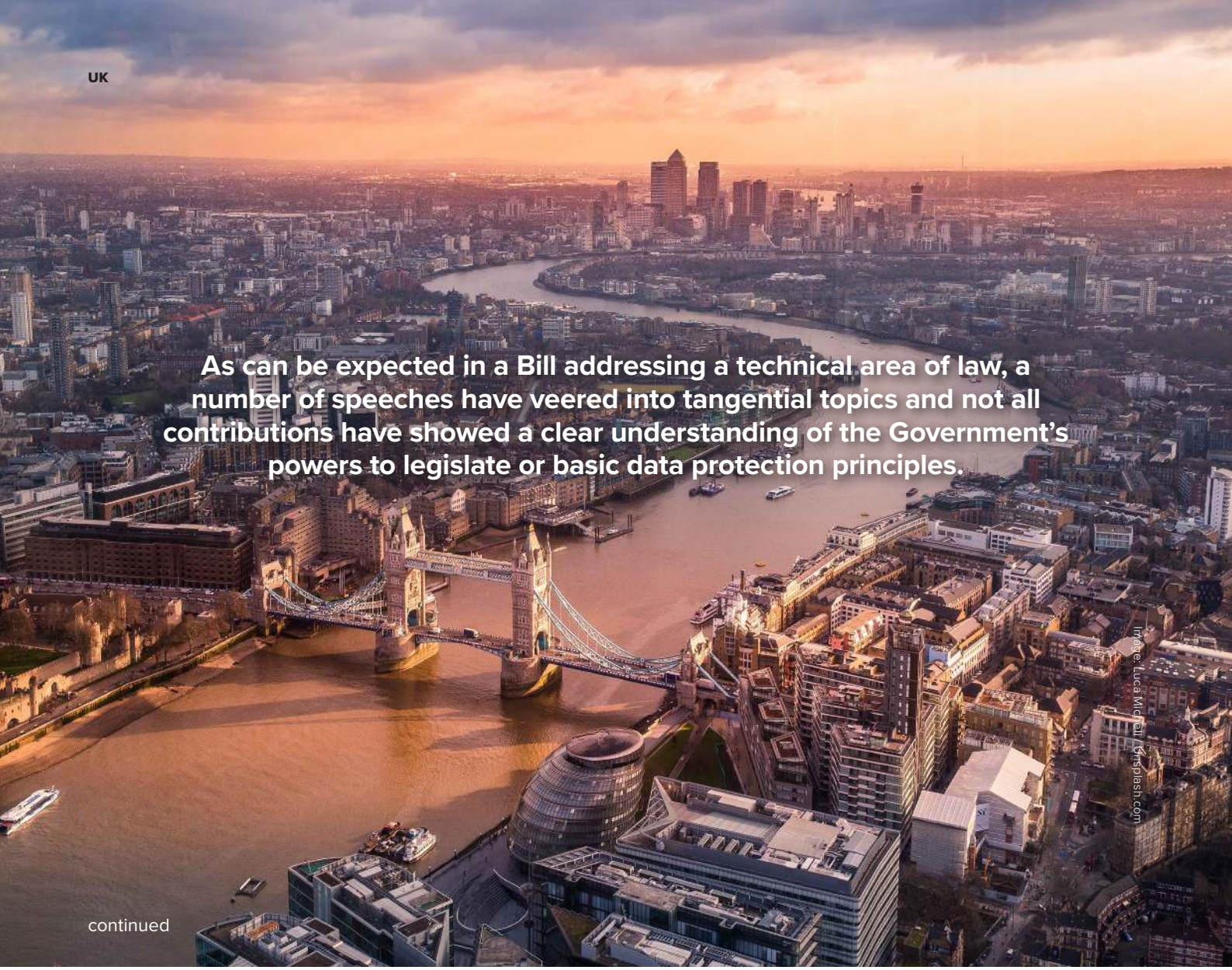
Part 3: Law enforcement
Implements the Law Enforcement Directive, wherever possible by building on the current data protection principles.

Associated schedules:
Schedule 7:
Lists the authorities to whom this Part applies.

Schedule 8:
Lists the additional conditions for processing sensitive personal data under the Law Enforcement Directive (a sub-set of Schedule 3 of the 1998 Act).

Part 4: National security
Rules for processing of personal data by intelligence services, much will be familiar from the 1998 Act.

Associated schedules:
Schedule 9:
Conditions for processing under Part 4 (equivalent to Schedule 2 of the 1998 Act).
Schedule 10:
Conditions for processing sensitive



As can be expected in a Bill addressing a technical area of law, a number of speeches have veered into tangential topics and not all contributions have showed a clear understanding of the Government's powers to legislate or basic data protection principles.

Image: Luca Micheli / Unsplash.com

continued

personal data (equivalent to Schedule 3 of the 1998 Act).

Schedule 11:
Exemptions to national security processing.

Part 5: Information Commissioner

Continued existence and functions of the ICO, including its international role, obligations to prepare codes of practice on data sharing and direct marketing. This Part also allows the ICO to require persons (other than data subjects and data protection officers) to pay for services provided and to require controllers to pay charges (i.e. notification fees in a new guise).

Associated schedules:
Schedule 12:
Appointment and funding rules, etc.

Schedule 13:
Functions of the ICO, including in relation to the GDPR and the Law Enforcement Directive.
Schedule 14:
Co-operation and mutual assistance provisions.

Part 6: Enforcement

Provisions relating to information notices, assessment notices, enforcement notices and penalties.

Rules relating to compensation and provisions on criminal offences. In addition to the offences in the 1998 Act, two new offences are introduced:

- an offence of re-identification of de-identified data is introduced; and
- an offence of altering personal data, after an access request has been received, with the intent of preventing disclosure of information to which the individual would otherwise have been entitled.

Associated schedules:
Schedule 15:
Powers of entry and inspection.

Schedule 16:
Procedural rules on penalties.

Part 7: Supplementary and final provisions

Carries forward current provisions relating to enforced subject access both generally and with specific reference to health records.

Continues current provisions relating to liability of directors and officers.

Associated schedules
Schedule 17:
Definition of relevant records (relevant to enforced subject access).

Schedule 18:
Minor and consequential amendments.

The initial skirmishes

The Government chose to introduce the Bill in the House of Lords, and the Bill's first reading - a purely formal stage - was held on 13 September 2017. A bill introduced in the Lords must progress through various rites of passage. It must survive a general high level debate at second reading, a more detailed committee stage where

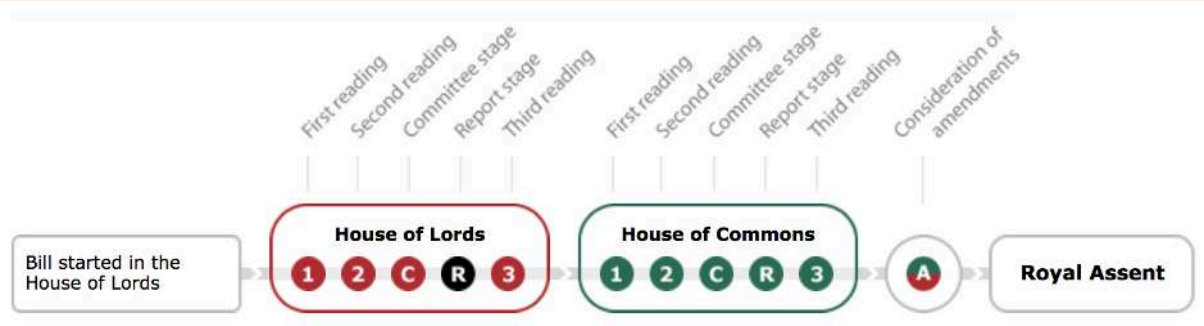


Figure 1: Passage of a bill through UK Parliament

amendments are first proposed and the Government is given a chance to explain its approach, a report stage where unanswered concerns of peers can be likely brought to a vote and a final third reading to sweep up outstanding administrative tweaks. It must then depart to run the same gauntlet through the House of Commons, before returning at last for the Lords' approval. Once approved by both houses, the Bill can progress to assent (see Figure 1).

The Bill entered its first day of the report stage on 11 December 2017. This followed a lengthy debate in the committee stage, where some 189 amendments were proposed with many of these being split or expanded into several parts.

A number of these were Government amendments, and indeed only those proposed by the Government were accepted – as is common practice at committee stage. Most of these amendments were effectively spring cleaning, although amongst the more substantive amendments was a procedure for creating a framework for data processing by the Government and new grounds for processing sensitive data in the areas of automated insurance renewals, publishing court decisions and sports governance.

In December, the Lords managed to progress through two days of the report stage. A further 217 amendments have been proposed, with the Government having faced three divisions, in each case avoiding defeat. As the Bill passes to the Commons, we can expect further pressure on certain questions. An opportunity to put the Government under pressure on Brexit saw one amendment pushed to the brink of an early vote. Labour and Liberal Democrat peers joined forces to push for an amendment that sought to insert the right to data protection contained in the European Convention of Human Rights ('the Convention') at the head of the Bill. This was triggered by the Government's refusal to include this Convention in the Withdrawal from the European Union Bill, currently running through the Commons. It was also prompted by a belief, in some quarters, that this would help bolster an adequacy application by the UK. The amendment was described by Lord Lester as "constitutionally illiterate[1]" and was not accepted. An attempt to revisit this issue in the report stage resulted in a victory for the Government, but the issue may still return in the Commons given its political importance.

Another battle being rehashed in the Lords was over the Leveson Report's recommendations on journalism. Unsurprisingly, given the subject matter, this was the only one to receive substantial press coverage at committee stage. Liberal Democrat peers were accused of trying to "hijack" the Bill by seeking to require compliance with the IMPRESS code, instead of the industry-preferred IPSO code[2]. A substantial amount of the report stage has been dedicated to reviewing journalistic exemptions and other media concerns, particular over criminal offences and ICO powers. The Government has attempted to address a number of these to avoid defeat, and has so far not lost a division over media matters.

The Government also made a substantial change at report stage to require the ICO to produce a third statutory code on the processing of children's data online. This has acted to avoid continued debate and challenge around the age at which children can consent to online services themselves, without verifiable parental consent being provided. The age was set by the Government at 13, but a number of peers had raised concerns that this was too simplistic.

The committee stage lasted for six sittings, and waded through a wide variety of issues and sectors. The report stage will continue into a third day on 10 January 2018. Although we have highlighted three areas of debate above, discussions have covered a myriad of special interests, from concerns over the scope of research exemptions, to a close vote on narrowing the anti-doping processing condition. As can be expected in a Bill addressing a technical area of law, a number of speeches have veered into tangential topics – such the law of confidence – and not all contributions have showed a clear understanding of the Government's powers to legislate or basic data protection principles.

The pace of progress - what happens next?

A problem faced by the Government as it headed into the report stage in the Lords was its lack of majority – should a matter unite Labour and the Liberal Democrats, it faced losing a vote. However, to date, the assistance of Unionist and crossbench peers has been sufficient to avoid defeat – although once by a margin of three votes. If any vote is lost in the new year on issues of substance, then the Government can overturn these in the Commons, where MPs will get sight of the Bill towards the end of January. This could push out the schedule – a disagreement between the houses can result in "ping-pong" between them to finalise approval. The Commons can eventually force a final say, but this may lead to some delay.

So far, the ongoing battle grounds appear to remain limited to Leveson and Brexit rather than genuine data protection concerns. It is not clear if there will be substantial battles on these points in the Commons. There is cross-party understanding that assent must come no later than May, given the impending deadlines - but that does not mean that the timetable won't go down to the wire.

Richard B. Newman Attorney
rnewman@hinchnewman.com
Hinch Newman LLP, New York

Complying with the FTC's COPPA rule in a data-driven world

Image: Anna Demianenko / Unsplash.com

The US Federal Trade Commission ('FTC') enforces the Children's Online Privacy Protection Act of 1998 ('COPPA'), which sets forth what operators of websites and apps must do to protect the online privacy and safety of children under 13 years of age. Richard B. Newman, Attorney at Hinch Newman LLP, provides a breakdown of the requirements under COPPA and what entities must know in order to lawfully collect the personal information of children.

The FTC's Division of Privacy and Identity Protection has been extremely active of late investigating and taking action against those that compromise the online privacy of children by failing to obtain parental consent before collecting their personal information. In fact, the FTC has brought more than 20 COPPA cases and collected millions of dollars in civil penalties. Of particular interest to the FTC are internet-connected or smart toys and other devices directed at children. COPPA is also vigorously enforced by state attorneys general.

Who must comply with COPPA?

Simply stated, COPPA applies to operators of websites and online services that collect personal information from children under 13. You must comply with COPPA if:

- your website or online service is directed to children under 13 and you collect their personal information;
- your website or online service is directed to children under 13 and you let others collect their personal information;
- your website or online service is directed to a general audience, but you have actual knowledge that you collect personal information from children under 13; or
- your company runs an advertising network or plug-in, for example, and you have actual knowledge that you collect personal information from users of a website or service directed to children under 13.

The broad definition of 'website or online service'

COPPA defines 'website or online service' broadly. In addition to standard websites, examples of others covered by COPPA include mobile apps that send or receive information online, such as network-connected games, social networking apps or apps that deliver behaviourally-targeted ads; internet-enabled gaming platforms; internet-enabled location-based services; Voice-over Internet Protocol ('VoIP') services; and connected toys or other Internet of Things devices.

'Directed to children under 13'

The FTC looks at a variety of factors to determine if a website or service is directed to children under 13, including the subject matter of the website or service, visual and audio content, the use of animated characters or other child-oriented activities and incentives, the age of models, the presence of child celebrities or celebrities who appeal to children, advertisements that are directed to children, and other reliable evidence about the age of the actual or intended audience.

If a website does not target children as its primary audience, but is 'directed to children under 13,' the operator may choose to apply COPPA protections only to users under 13. In such cases, operators are proscribed from collecting personal information from users without first collecting age information. Moreover, the FTC makes clear that operators must not collect any personal information from users that say they are under 13 until verifiable parental consent has been obtained.

Definition of 'personal information' and 'collect'

Under COPPA, personal information includes:

- full name;
- home or other physical address,

If another company collects personal information through a child-directed site or service, such as through an advertising network or plug-in, the operator is responsible for complying with COPPA.

including street name and city or town;
- online contact information like an email address or other identifier that permits someone to be contacted directly;
- screen name or user name where it functions as online contact information;
- telephone number;
- social security number;
- a persistent identifier that can be used to recognise a user over time and across different sites, including a cookie number, an IP address, a processor or device serial number, or a unique device identifier;
- a photo, video, or audio file;
- sufficient geolocation information to identify a street name and city or town; and
- other information about the child or parent that is collected from the child and is combined with one of these identifiers.

Under COPPA, collection includes requesting, prompting or encouraging the submission of information, even if it is optional; letting information be made publicly available (for example with an open chat or posting function) unless the operator takes reasonable measures to delete all or virtually all personal information before postings are public and deletes all information from its records; or passively tracking a child online.

If another company collects personal information through a child-directed site or service, such as through an advertising network or plug-in, the operator is responsible for complying with COPPA. If the operator possesses actual knowledge that it is collecting personal information directly from users of a child-directed site or service, the operator is also responsible for complying with COPPA.

Privacy policies

If covered by COPPA, operators must post a clear and conspicuous privacy policy that thoroughly describes how personal information collected online from children under 13 is handled. The privacy policy must describe both the operator's practices and the practices of any others collecting personal information on the website or service.

A link to the privacy policy should be posted on the homepage and anywhere personal information is collected from children. General audience websites or services that possess a separate section for children should include a link to the privacy policy on the homepage of the children-designated portion thereof.

Links to privacy notices should be prominent, in a larger font or different colour type on a contrasting background. A mouseprint link at the bottom of the page – below the fold – that is not distinguishable from other links will not suffice.

The FTC recommends that privacy policies be simple to read and include, without limitation, a list of all operators collecting personal information, along with names and contact information; a description of the personal information collected, and how it is collected and used; and a description of parental rights and the procedures to follow to exercise their rights.

Providing parents with direct notice of information practices

COPPA requires that operators provide parents with 'direct notice' of information practices before collecting information from their children. In addition, material changes to previously agreed to practices require updated notices.

The notices must include, without limitation, that online contact information has been collected for the purpose of getting their consent; that the operator wants to collect personal information from their child; that their consent is required for the collection, use and disclosure of the information; the specific personal information the operator wants to collect and how it might be disclosed; a link to the online privacy policy; how the parent can provide consent; and that if the parent does not consent within a reasonable time, the operator will delete their online contact information from its records.

In certain circumstances, it may be acceptable to collect a narrow class of personal information without obtaining parental consent. However, parents must still be provided with direct notice of the activities.

The requirement of 'verifiable consent'

Prior to collecting, using or disclosing personal information from a child, verifiable parental consent is required. This is a key component of COPPA.

According to FTC guidance, the method chosen must be reasonably designed in light of available technology to ensure that the person providing the consent is the child's parent. If the operator has actual knowledge that it is collecting personal information from a website or service that is directed to children, it may obtain consent directly or through the child-directed website or service.

The FTC has stated that acceptable methods include having the parent sign a consent form and send it back via fax, mail or electronic scan; using a credit card, debit card or other online payment system that provides notification of each separate transaction to the account holder; calling a toll-free number staffed by trained personnel; connecting to trained personnel via video conference; providing a copy of a form of government-issued ID that is checked against a database, as long as it is deleted when the verification process is completed; answering a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer; or verifying a picture of a driver's licence or other photo ID submitted by the parent and then comparing that photo to a second submitted photo using facial recognition technology.

If a child's personal information will only be used for internal purposes and will not be disclosed, the operator may use a method known as 'email plus.' An email is sent to the parent with a request to respond with consent. The operator must send a confirmation to the parent via email, letter or telephone call. The parent must also be advised that they can revoke consent at any time. Moreover, the parent must be provided with the option of allowing the collection and use of their child's personal information

If covered by COPPA, operators must post a clear and conspicuous privacy policy that thoroughly describes how personal information collected online from children under 13 is handled. The privacy policy must describe both the operator's practices and the practices of any others collecting personal information on the website or service.

continued

without agreeing to the disclosure of that information to third parties.

Parents' ongoing rights

Even if parents have agreed to the collection of their child's information, they have ongoing rights and operators have continuing obligations.

If a parent asks for it, the operator must provide a way to review the personal information collected from their child; a way to revoke consent and refuse the further use or collection of personal information; and must delete the personal information.

Importantly, any time an operator communicates with a parent about personal information already collected from their child, reasonable steps must be taken to ensure that the operator is, in fact, dealing with the child's parent. Additionally, methods utilised to provide parents access to information collected from their children cannot be unduly burdensome on the parent.

Reasonable procedures to protect personal information

COPPA requires that reasonable procedures to protect the confidentiality, security and integrity of personal information be established and maintained. Operators should minimise what is collected and personal information should only be released to service providers and third parties capable of maintaining its confidentiality, security and integrity. In addition, operators should obtain written assurances that such third parties will live up to those responsibilities, and personal information should be retained only as long as is reasonably necessary for the purpose for which it was collected, and should be disposed of once there no longer exists a legitimate reason for its retention.

COPPA's application to voice recordings

The FTC recently provided additional guidance on how COPPA applies to the collection of audio voice recordings. In an October 2017 policy enforcement statement, the FTC noted that the COPPA rule requires websites and online services directed at children to obtain verifiable parental consent before collecting an audio recording. In doing so, the FTC expressed its recognition of the value of using voice as a replacement for written words in performing search and other functions on internet-connected devices.

The FTC stated that it will not initiate an enforcement action against an operator for not obtaining parental consent before collecting an audio file with a child's voice when it is collected solely as a replacement of written words, such as to perform a search or to fulfil a verbal instruction or request, as long as it is held for a brief time and only for that purpose.

There are, of course, important limitations to this policy. It does not apply when the operator requests information via voice that would otherwise be considered personal information, such as a name. In addition, an operator must still provide clear notice of its collection and use of audio files and its deletion policy in its privacy policy.

Also, the operator may not make any other use of the audio file before it is destroyed and the policy does not affect the operator's COPPA compliance requirements in any other respect.

Noteworthy COPPA enforcement actions and trends

In 2016, a Singapore-based mobile advertising company paid $950,000 in civil penalties and was required to implement a comprehensive privacy programme to settle FTC charges that it deceptively tracked the locations of hundreds of millions of consumers, including children, without their knowledge or consent, to serve them geo-targeted advertising. The FTC alleged that the company misrepresented that its advertising software would only track consumers' locations when they opted-in and in a manner consistent with their device's privacy settings. According to the FTC, the company was tracking consumers' locations regardless of whether the apps using the software asked for their permission to do so, and even when consumers had denied permission to access their location information.

The FTC also recently reached a settlement with two app developers that allowed third-party advertisers to collect information about children without parental consent. The developers paid a combined $360,000 in civil penalties for alleged COPPA violations. This settlement is noteworthy because it was the first in which the FTC alleged that companies allowed advertisers to use persistent identifiers – pieces of data that are tied to a particular user or device – to advertise to children. Persistent identifiers were among the categories added to COPPA's definition of personal information when it was updated in 2013.

Child advocacy and privacy groups have recently called on the FTC to investigate several smartwatch brands and the privacy risks they pose to children. The advocacy groups, including the Electronic Privacy Information Center, the Center for Digital Democracy and the Consumer Federation of America, claim that some of the popular smartwatch models are hackable. The FTC has clearly evidenced a willingness to aggressively scrutinise compliance with COPPA and data security issues related to the Internet of Things.

Ivan Dario Marrugo Jimenez Partner and CEO
imarrugo@marrugorivera.com

Andres Felipe Contreras Poveda Associate Consultant

acontreras@marrugorivera.com

Marrugo Rivera & Asociados: FuturLex, Colombia

Cross-border data transfers under the Colombian data protection regime

In August 2017, the Colombian data protection authority ('SIC') issued Circular No. 05 of 2017, which develops the regulation of cross-border data transfers in Colombia ('the Circular'), following consultations held in February and July to seek comments on the criteria SIC should use to determine which countries provide an adequate level of data protection. Ivan Dario Marrugo Jimenez and Andres Felipe Contreras Poveda, Partner & CEO and Associate Consultant at Marrugo Rivera & Associates - FuturLex respectively, analyse the Circular and what it means for the transfer of personal data outside of Colombia.

Determining adequacy

By approving the Circular, SIC took one of the most controversial decisions in years related to data protection, not only in Colombia but internationally, by declaring that the US provides an adequate level of data protection. Independently of the criticism that this decision has led to, SIC has prepared a regulatory model with a series of provisions to reinforce the obligations that derive for data controllers and processors from the transfer and transmission of personal data to third countries.

In this context, the Circular sets out the standards used to determine which countries provide a high or adequate level of personal data protection, in order to verify that a transfer or transmission can be carried out lawfully, without any additional burden or requirement beyond that of observing whether the country of destination of the personal data is contained in the list included in the Circular ('the Adequacy List').

Subsequently, the Circular states that when the transfer of personal data will be made to a country that is not in the Adequacy List, it will be the responsibility of the data controller to verify if the country to which the data is being transferred meets the established standards. If the recipient country does not comply with the standards, the controller will have to request a declaration of conformity from SIC in order to transfer the data.

These standards, included in Section 3.1 of the Circular, are the following:

- the existence of rules applicable to personal data processing;
- normative recognition of principles applicable to data processing, such as legality, purpose, freedom, veracity or data quality, transparency, access and restricted circulation, security and confidentiality;
- regulation of data subject rights;
- regulation of the duties of data controllers and data processors;
- existence of judicial and/or administrative means and channels to guarantee the protection of the rights of data subjects and to demand compliance with the law; and
- existence of supervisory authority/ies for personal data processing, compliance with applicable legislation and the protection of the rights of data subjects.

International transmissions of personal data

At this point, it is pertinent to make a series of observations and comments on the position that Colombian legislation has taken with regard to the concepts of 'transmission' and 'transfer,' in the face of the model the Circular creates.

Article 24(2) of Decree 1377 of 2013 (June 27) Which Partially Regulates Law 1581 of 2012 ('the Decree') provides that international transmissions of personal data between a data controller and a data processor to allow the processor to perform the processing on behalf of the data controller, shall not require the data subject to be informed or to give their consent when there is a contract under the terms of Article 25.

The abovementioned article mirrors Article 2.2.2.25.5.2 of Decree 1074 of 2015, mentioned in the Circular. According to this provision, the international transmission of data between a data controller and data processor may be of two types, contractual or extracontractual. Extracontractual transfers must be authorised by the data subject.

By virtue of the contractual relationship illustrated in Article 25 of the Decree, data controllers and data processors are responsible for, respectively, the following:

- indicating the scope of the processing, the activities the processor will perform on behalf of the controller

Image: Jenner Images / Moment / Getty Images

By approving the Circular, SIC took one of the most controversial decisions in years not only in Colombia, but internationally, as regards the postulates of data protection, by declaring that the US is a country that provides an adequate level of data protection.

continued

for the processing of the personal data, and the obligations of the data processor with regard to the data subject and the data controller; and
- committing to complying with the controller's obligations under the data processing policy the controller has set out and performing the data processing in accordance with the purposes the data subjects have authorised and with applicable laws.

In addition, among other duties, the Decree specifies the following obligations for data processors:

- to process, on behalf of the data controller, personal data in compliance with the principles that safeguard them;
- to safeguard the security of the databases containing personal data; and
- to maintain confidentiality regarding the processing of personal data.

Having said that, it should be clarified that the exemption regarding the obligation to inform and obtain authorisation from data subjects referred to in Article 24(2) of the Decree, unlike the contractual requirements contained in Article 25, alludes not to the information on, and consent to, the processing itself, but specifically, to the sending of personal information that will be processed by a third party through the international transmission of data. Now, as indicated in the Circular, regarding the instructions for the international transmission of personal information if there is no transmission contract, one of the following rules must be complied with:
• informing the data subject of the transmission of the data and obtaining their authorisation for it; or
• observing the provisions of Article 26 of Statutory Law 1581 of 2012 (October 17) Which Issues General Provisions for the Protection of Personal Data ('the Data Protection Law').

Article 26 of the Data Protection Law refers to the general prohibition not to transfer personal data of any kind to countries that do not provide adequate levels of data protection, subject to a list of exceptions.

Equally, it is pertinent to mention that, except for the special characteristics of the concepts of transfer and transmission which are ultimately a result of the qualities that distinguish the figures of controller and processor in terms of the power of decision-making, control and direction that the former has over the latter the only difference present in the Data Protection Law and the Decree, is the transmission contract contained in Article 25 of the Decree.

Conclusions

The following conclusions can be put forward after analysing the Circular. Firstly, the reference made by the Circular to Article 26 of the Data Protection Law, rather than revealing a protectionist character, since it equates the regulation of transmissions with that of transfers, may mean that SIC, to some extent, did not fully understand the will of the legislator. If the latter had wanted the provisions that are exclusive to one figure to apply to the other, it would not have bothered to make such a categorisation, nor assign specific articles to each.

Secondly, the concept of unauthorised international transfers, previously supported exclusively by the existence of a contract between the data controller and the data processor that is clearly intended to assign the competences, obligations and responsibilities of both parties, is now much broader. This is the case since such transmissions can be carried out on one of the grounds set forth in Article 26 of the Data Protection Law, on the basis of a declaration of conformity issued by SIC beforehand, or if the transmission is to one of the countries listed in Section 3.2 of the Circular.

Thus, although SIC sought to relax the issue of transmissions in favour of data controllers, this may lead to, correlatively, additional issues, by depriving personal data of a protection tool, which is the contract of transmission of personal data contained in Article 25 of the Decree.

Márton Domokos Senior Counsel, Co-ordinator of CEE Data Protection Practice
marton.domokos@cms-cmno.com

CMS Cameron McKenna Nabarro Olswang LLP Magyarországi Fióktelepe, Budapest

Valentina Parvu Senior Associate
valentina.parvu@cms-cmno.com

CMS Cameron McKenna Nabarro Olswang LLP, Bucharest

Ksenija Ivetić Marlović Senior Attorney
ksenija.ivetic@cms-rrh.com

Petrikić & Partneri AOD, Belgrade

Andrea Cervenkova Associate
andrea.cervenkova@cms-cmno.com

CMS Cameron McKenna Nabarro Olswang, advokáti, v.o.s., Czech Republic

Angelika Sedlackova Senior Associate
angelika.sedlackova@cms-cmno.com

CMS Cameron McKenna Nabarro Olswang LLP, Bulgaria

Martina Novysedlakova Associate
martina.novysedlakova@cms-cmno.com

CMS Cameron McKenna Nabarro Olswang, Slovakia

Central and Eastern Europe round-up: enforcement decisions and major developments

When planning business operations in Central and Eastern Europe ('CEE'), data protection law is as important as any other area of law. Most business projects will involve some processing of personal data, whether that of employees, customers or potential clients. In fact, personal data protection rules will potentially apply in any scenario where information relating to an individual is involved in any way. Although the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') is harmonising the data protection laws also in the CEE, local laws will continue to apply, e.g. in employment-related data processing, cybersecurity, and cookie compliance. Angelika Sedlackova, Andrea Cervenkova, Márton Domokos, Valentina Parvu, Ksenija Ivetić Marlović and Martina Novysedlakova from CMS Cameron McKenna Nabarro Olswang, discuss the most relevant enforcement decisions and developments that have recently taken place in Bulgaria, the Czech Republic, Hungary, Romania, Serbia and Slovakia, and which must be taken into account by companies operating in such jurisdictions.

Bulgaria

For the first time since its creation, in 2016, the Commission for Personal Data Protection ('CPDP') conducted a comprehensive sector compliance examination, which concerned the education sector and included 4,611 educational institutions of various kinds. Among other mandatory instructions to the monitored educational institutions, the CPDP expressly prohibited kindergartens to request and store copies of birth certificates of applicant children.

In addition, a number of verifications were executed by the CPDP at the end of 2016 regarding presidential elections and a national referendum, both held in November 2016. The subject of concern was the processing of personal data by political parties and coalitions gathered via signature subscriptions. Six parties, three coalitions and 12 initiative committees were sanctioned for processing personal data without proper registration with the CPDP. Further, at the end of 2016, the CPDP issued its decision in a case related to personal data processed by the National Revenue Agency ('NRA'). The CPDP established that, when it revealed personal data of an individual subject to a NRA verification to third parties and in notifications addressed to them for collection of documents, the NRA violated the prohibition to conduct additional processing in a manner incompatible with the purpose of processing. The NRA was sanctioned with BGN 10,000 (approx. €5,110).

In March 2016, the CPDP addressed a case related to the powers of private bailiffs in Bulgaria. A well-known private bailiff in Sofia was imposed a pecuniary sanction of BGN 10,000 for the following violation: he processed personal data of an individual who participated in the enforcement case in his capacity as a mortgage (not main) debtor. The CPDP ruled that under the enforcement procedure a mortgage debtor participates to the extent that enforcement actions may be initiated towards the mortgaged real estate, not only towards the mortgage debtor himself. Gathering data for the economic status of the mortgaged debtor was found illegal.

A recent media case saw the CPDP imposing a sanction of BGN 15,000 (approx. €7,670) to the owner of a news oriented internet site for publishing a politician's personal data. The defendant based its arguments on the freedom of speech and information of society principles. Nevertheless the CPDP ruled that said principles would not be violated if sensitive personal data was properly deleted.

Another interesting case related to a company providing test drive services, which required to be presented with copies of identity cards and driving licences of its customers. The CPDP

continued

ruled that the requirement for a driving licence corresponded to the provided service, but the requirement to provide the identity card was incompatible with the purpose of processing. The test drive company was sanctioned with BGN 12,000 (approx. €6,130).

The highest sanction imposed by the CPDP amounted to BGN 63,000 (approx. €32,210) and was imposed to Sofia Water Supply company for providing personal data of its customers to a debt collecting company without proper prior consent.

Czech Republic

Unsecured client personal information stolen by an employee

The Office for Personal Data Protection of the Czech Republic ('UOOU') issued a fine of CZK 3,600,000 (€144,000) to T-Mobile Czech Republic for the theft of client personal data by a T-Mobile employee. The UOOU held T-Mobile was responsible for not having the personal data of clients within its electronic database properly secured. The stolen data included names, dates of birth, bank accounts and information on telephone plans or average spending. The former employee was also being prosecuted criminally.

Highest fine for spam

The highest data protection penalty issued in 2017 was a fine of CZK 4,250,000 (€170,000) to EURYDIKAPOL, s. r. o. (also known as JH HOLDING s. r. o.). This has also been the highest fine issued so far for unsolicited commercial messages. The spam was sent out repeatedly over a year, with the company being unable to prove consent of the receivers to such messages. The fact that the company continued the unlawful practice even during the investigation, as well as the large amount of messages (in one case a receiver was sent nearly 200 messages) sent was partially the reason for the amount of the fine.

Posting a picture of a shoplifter on Facebook

The UOOU published an official statement after the Czech Constitutional Court ruled on the infamous case of the company ekolo.cz sro. In this case, an electric bicycle was stolen by a shoplifter, who was recorded by a security camera in the shop. When police were unable to find the offender even when provided with a clear picture of him as recorded by the camera, the shop owner published the photograph on Facebook asking the public for help. As the status went viral, with help of the public, the shoplifter was identified, caught by police and criminally prosecuted.

However, the UOOU fined the shop owner for violating the rights of the later convicted shoplifter by posting his picture on Facebook. While this legal opinion has been approved by the courts of appeal and by the Constitutional Court, the UOOU itself, with its new director, later stated this would not have been opined, and that such a strictly formal application of law is unjust.

Hungary

Copying IDs, form of consent and contacting the customers' employer

In Hungary, the National Authority for Data Protection and Freedom of Information ('NAIH'), imposed a HIF 1,000,000 fine (approx. €3,200) on a company whose business was selling and managing a wide range of financial services, including consumer credit, payment solutions, loan redemption and banking services. Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information ('the Info Act') provides that companies can process personal data only for specified and explicit purposes, where it is necessary for the implementation of certain rights or obligations.

The purpose of processing must be satisfied in all stages of data processing operations; recording of personal data shall be done under the principle of lawfulness and fairness. The NAIH declared that individuals shall provide personal data only if such data are necessary for concluding, performing or terminating the financial services agreements, and it is the financial services provider who shall prove that these criteria are fulfilled. The NAIH found that making copies of ID cards of customers who appeared at the financial service provider in person is excessive, even if the customers provide their prior consent to such practices. The NAIH argued that the financial service provider shall identify the customer once he/she has shown the ID, and that it is not necessary to make and store a copy of it as well, since a copy will not have any probative force (compared to the original document).

The NAIH also reviewed other consent forms used by the company and found that it was not enough to indicate 'direct marketing' as a data processing purpose: the privacy information notice provided should contain the exact use of such data, including marketing as well. Moreover, the NAIH claimed that it may be enough to use anonymised information for product development statistics, and such purpose does not require the use of the actual personal data of customers.

Image: Zoltan Tasi / Unsplash.com

In regard to data protection law, NAIH accepts that blockchain users may carry out data processing in various jurisdictions. In these cases, it proposes that companies should identify the country where the data is being processed.

As regards the verification of customers' income, the NAIH declared that the financial services provider could contact the customer's employer only upon the prior - preferably written - consent of the customer. The customer shall provide his/her consent separately for each data processing purpose, and the privacy notice shall specify the list of personal data that the financial services provider can process. It is unlawful if the privacy notice states that the financial services provider can obtain any personal data from the customer's employer or other bank.

Prize draw competitions and personal data

Further, the NAIH imposed a HIF 1,000,000 fine (approx. €3,200) on an insurance company who offered a prize draw competition for its customers without providing adequate privacy information. For example, the NAIH found that the privacy notice pertaining to the competition did not contain a detailed list of the data processors involved, including their specific activity and for how long they could access the participants' data. The NAIH also looked into the mandatory registration of the company in the Data Protection Registry and found that the content of the registration did not match the information provided in the privacy notice in many respects, such as the scope of data, the processing purpose and the data retention period. The privacy notice did not contain detailed information on the participants' data protection rights and remedies either, e.g. the deadlines applicable for the company to fulfil the individuals' requests, and indication of the competent court. The NAIH also ordered the insurance company to obtain a separate consent for the transfer of personal data to another member in its company group (who would send marketing messages) and conclude a data transfer agreement for this purpose. The insurance company was required to publish the privacy notice on its website.

Data protection aspects of blockchain

Recently, the NAIH issued guidance on blockchain and data protection. The guidance answers the questions of a private individual in a specific case, and the NAIH published it due to public interest and the rise of the technology. The guidance provides a short description of blockchain technology, defines personal data, the legal bases of data processing, and how to identify the data controller and data processor in the blockchain.

According to the NAIH, blockchain is a decentralised network where no central entity controls system functions and transactions executed with the data. Each user is engaged in data processing, and each person who adds blocks and personal data to blocks in the system is a data controller. Subsequent users may later add personal data to the system and obtain an exclusive right to dispose of their data stored in blocks. In this case, they can execute a transaction using the data. As a result of a transaction, if the right to dispose of personal data stored in the block is transferred to another user (i.e. the recipient of data who will have the exclusive right of disposal), the NAIH considers this user a data controller.

While it provides practical guidance on how to identify the data controllers and data processors in the blockchain, the NAIH does not address how FinTech companies can follow this approach in the case of a large blockchain, and in particular compliance with Privacy by Design obligations. Moreover, the NAIH does not go into detail about technical solutions (e.g. data access management platforms) to address the complex obligations of FinTech companies to demonstrate that they are compliant when processing data in the blockchain.

In regard to data protection law, the NAIH accepts that blockchain users may carry out data processing under various jurisdictions. In these cases, it proposes that companies should identify the country where the data is being processed. This would be the country where the data controller is carrying out the actual data processing operations. (i.e. where he/she places a transfer order, accesses and adds data to the blockchain, mines bitcoin, or issues orders to carry out operations). The NAIH confirms that the physical location of the data in the blockchain is irrelevant, but states that the Court of Justice of the European Union ('CJEU') approach in the *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (C-131/12) would also apply. While the examples provided by the NAIH are a good starting point for FinTech companies to determine what laws are applicable to their operations, the GDPR will also have a major impact on the industry.

Regarding the question whether the long-term use of blockchain makes users and their patterns of behaviour vulnerable to monitoring and profiling, the NAIH states this risk depends on the characteristics of a specific

Serbia has been waiting for the new personal data protection law for over two years. Personal data protection is one of the topics of chapters 23 and 24 of Serbia's accession negotiations with the EU.

continued

system, the data processed in it, and its auxiliary data processing operations.

In conclusion, the NAIH guidance is highly important since Hungary has a dynamic privacy-sensitive FinTech scene. The NAIH touches key points of the data protection obligations of companies, but it is clear that market players and users expect more detailed sector-specific guidance in the following areas: Privacy by Design, subject access rights, data retention, data reversibility, data security, and transparency obligations.

Romania

In anticipation of the entry into force of the GDPR, the Romanian Ministry of Internal Affairs launched, on 5 September 2017, for public debate, a bill for the amendment of the current legislation on the organisation of the National Supervisory Authority for Personal Data Processing ('ANSPDCP') and for the abrogation of the current Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data.
The main purpose of the draft legislation is to enhance the administrative and institutional capacity of the ANSPDCP (currently considerably under-staffed and under-budgeted) so that the ANSPDCP can effectively cope with its role and new attributions of control and safeguard of the rights of the EU citizens, as enriched in the GDPR.

The draft legislation also aims to set out a unitary and detailed framework for the performance by the ANSPDCP of its powers of control, in particular with regard to the conduct of investigations and the solving of complaints.

The following are worth mentioning:

- The ANSPDCP is entrusted with large powers of control of data controllers and their empowered persons, including via impromptu investigations, request of information, witness interviews, and access to the locations and the equipment where data is stored (note: the ANSPDCP would need a court approval to conduct such investigations only in the situation that the personnel entrusted with the control mission would encounter obstacles from those investigated).
- The actions available to the ANSPDCP to ensure compliance are classified as 'corrective measures,' recommendations and cease orders by the courts (in the latter case, the data subject automatically becoming a plaintiff). The corrective measures include administrative sanctions (i.e. fines and warnings; other measures include prohibition of processing, erasure of the data, suspension of data flow towards a third country).
- There is a proposed threshold of €300,000 as a fine, above which the attribution to apply the fine rests exclusively with the President of the ANSPDCP (also, if a fine larger than the RON equivalent of €300,000 is being considered, the ANSPDCP is required to issue, in addition to minutes of the investigation, an investigation report, which normally includes significantly more information than the minutes, and is comprehensive of the defence of the controlled entity).
- Note, the fine is to be paid within a term of 15 days (the position of the ANSPDCP's representative as further reflected in the draft legislation is that the right - under the common administrative contentious rules - to pay half of the amount of an administrative fine if payment is made within 24 hours from the sanctioning would not apply in this context).
- The data controller/empowered person is entitled to challenge the relevant administrative deed of the ANSPDCP before the competent tribunal within 15 days from communication, with the possibility to further appeal the tribunal's decision before the Court of Appeal (no term is provided so far). Note, the challenge does only suspend the payment of the fine, not the other measures that may have been imposed.

Serbia

Serbia has been waiting for its new personal data protection law for over two years. Personal data protection is one of the topics of chapters 23 and 24 of Serbia's accession negotiations with the EU. Earlier this year, the Commissioner for Information of Public Importance and Personal Data Protection prepared a draft law ('the Draft Law'), which was put to public debate. Following the debate and finalisation of the wording of the Draft Law, this was forwarded to the Ministry of Justice for further action. On 14 November 2017, the Minister of Justice Ms Nela Kuburović announced that the Draft Law will soon be available for public debate. However, at the time of publication, the Draft Law is still not publicly available.

Slovakia

The Office for Personal Data Protection of the Slovak Republic ('PDP') does not regularly publish statements or comments on specific cases once an investigation is completed. Instead, it publishes bi-annual reports providing statements on a number of selected significant cases.
In 2016, the highest fine issued by the PDP was €7,000 (whereas the average fine was €2,130) for collecting biometric information without a reasonable purpose. However, detailed information on the case has not been disclosed.

The PDP also investigated an employer who installed GPS tracking devices into cars employees were using, not only for business purposes, but also during their spare time as a form of fringe benefit. During the investigation, it was made clear that the employer was gathering information on location and movement of the employees outside working hours, for which there was no legal reason to do so and thus such behaviour was considered unlawful. No fine was issued as the employer ceased the practice upon notice by the PDP.

Michael Park Partner
michael.park@allens.com.au

Leah Wickman Associate
leah.wickman@allens.com.au

Allens, Melbourne

Managing risk in light of Australia's new National Digital Health Strategy

Image: Colin Rex / Unsplash.com

In an effort to transform the quality and sustainability of healthcare, Australia has introduced a National Digital Health Strategy aimed at evolving the healthcare industry by effectively using digital information. In this article, Michael Park and Leah Wickman, Partner and Associate at Allens respectively, examine Australia's introduction of a nationalised electronic health record system, the risks and what this step might mean for the healthcare industry.

Introduction

Digital forms of communication and information have changed how consumers, businesses, and governments interact. Time and space are no longer detriments to the flow of information, with information becoming immediately accessible regardless of one's location. However, when it comes to health information, there has been slow adoption of digital information. While there has been innovation in the industry, such as new forms of communication between healthcare professionals and patients, patients' health information has not evolved to meet the demands of a digital world.

eHealth globally: is this new?

The Australian Federal Government's push for eHealth follows a number of similar initiatives across the globe. In countries such as Canada and the UK, there have been a number of studies and surveys conducted to explore the increased use of digital technologies to support the delivery of healthcare services. However, only Singapore, and now Australia, have taken concrete steps to implement nationalised electronic health records.

Australia's Strategy is similar in many ways to Singapore's National Electronic Health Record ('NEHR'). Both attempt to implement nationalised electronic health records are aimed at increasing the quality of healthcare services by allowing greater accessibility to health information. Similar to Australia, the NEHR automatically enrols patients and provides them with an opt-out option.

The NEHR shows how quickly and widely electronic health information may be adopted in Australia. According to the Singaporean Ministry of Health, since the NEHR was introduced in 2013, usage has increased exponentially. As of April 2017, in excess of 21,000 healthcare professionals from more than 1,000 healthcare providers have access to the NEHR. This includes healthcare providers from the private sector, such as specialist clinics, X-ray labs, dental clinics, pharmacies and more[1].

However, Singapore's example has shown how difficult it is to convince all health providers to join a nationalised electronic health record system. While all public healthcare institutes are using the NEHR, private institutions have not shown great interest. This is problematic, as patients tend to visit both public and private healthcare providers, therefore curtailing the benefits of the NEHR. Private healthcare providers have expressed concerns regarding the cybersecurity and privacy of patients.

While the Singaporean Government continues to negotiate with private healthcare providers, reports indicate that the Ministry of Health is considering making it mandatory to participate in the NEHR.

For Australia, the Singaporean example will be closely watched to ensure that the majority, if not all, of healthcare providers actively use and contribute to the Australian electronic health record regime. The Australian Federal Government will also be considering the risks associated with electronic health information, such as the potential for data breaches and general privacy concerns.

eHealth in Australia

Healthcare in Australia

Australia has a system of both nationalised and private healthcare. Australian citizens and permanent residents (collectively, 'Australians') can access the publically funded national healthcare scheme, known as Medicare. Medicare can be supplemented or replaced by private health insurance. Private health insurance allows holders to access the private health sector, including private hospitals.

Those living in Australia that do not have citizenship or permanent residency are ineligible for Medicare and private health insurance is mandated. The eHealth initiatives discussed below will not apply to those ineligible for Medicare.

Australian eHealth initiatives

In July 2012, the Federal Government first introduced its plan to significantly reshape the Australian healthcare sector by allowing both Australians and healthcare providers to access and share health records electronically

1. https://www.moh.gov.sg/content/moh_web/home/pressRoom/Parliamentary_QA/2017/national-electronic-health-record.html

continued

through the introduction of the Personally Controlled Electronic Health Records Act 2012 (Cth) ('the PCEHR Act').

The implementation of the eHealth record system was intended to vastly improve the efficiencies of the Australian healthcare system, reduce the occurrence of adverse medical events and also benefit patients by providing more personalised and predictive healthcare. Issues arose with this initial attempt at effecting an eHealth record system, principally because the system was implemented on an opt-in basis, which resulted in limited uptake and as a result limited success.

In 2013, the Federal Minister for Health announced a review of the PCEHR system by a panel of health and IT experts. The panel made 38 recommendations, including:

- establishing new governance arrangements;
- moving to an opt-out system for participation; and
- improving system usability and the clinical content of records.

In 2015, the PCEHR Act was amended to respond to the review. Amendments included rebranding 'personally controlled electronic health record' as 'My Health Record' ('MyHR') and renaming the act to the My Health Records Act.

The National Digital Health Strategy

In 2016, the Australian Digital Health Agency ('ADHA') was established by the Australian State and Territory Governments. The ADHA's primary responsibility is to evolve digital health capability through leadership, collaboration and innovation in order to facilitate digital health integration in the health system.

The ADHA was also tasked with developing a National Digital Health Strategy ('the Strategy') that could support the public and private digital health planning and investment already occurring throughout Australia. The development of the Strategy was underpinned by several guiding principles, including ensuring privacy and security, and driving a culture of safety and quality.

The ADHA undertook an extensive consultation period in developing the Strategy, consulting key stakeholders including consumers, healthcare providers and professional bodies. The Council of Australian Governments Health Council approved the Strategy on 4 August 2017.

The Strategy aims to improve the quality and accessibility of healthcare services by achieving seven strategic priority outcomes by 2022. The seven strategic outcomes all revolve around the use of digital information and digital forms of communication to provide Australians with high quality healthcare and include:

- health information that can be exchanged securely;
- digitally-enabled models of care that drive improved accessibility, quality, safety and efficiency; and
- a thriving digital health industry delivering world-class innovation.

Currently, MyHR (the secure online summary of patients' health information) is used by over five million Australians. Under the Strategy, all Australians will automatically be signed up to MyHR by the end of 2018 unless they opt-out.

By 2022, all healthcare providers will be able to contribute to and use health information in a patient's MyHR, providing instantaneous access to health information regardless of the health provider's location. As a result of the improved access to health information, such as allergies, medical conditions, history of treatments, medicine details and more, health professionals and services will no longer work in isolation.

The Strategy will likely result in innovation and improvement in the healthcare industry. Most immediately, MyHR will provide an opportunity for patients and healthcare providers to interact in a new way: remotely, using technology, rather than face-to-face. Australia has many communities living in rural and often isolated areas, and this flexibility of contact could vastly improve their quality of life.

Managing the risks

While the Strategy represents an ambitious and forward-thinking approach to eHealth data management, there is never reward without some risk.

Data breach

For many Australians, the use of MyHR raises privacy concerns, particularly due to the high sensitivity of health information. Such concerns are valid given that data breach incidents, both accidental and malicious, have struck both public and private health providers in Australia in recent years. For example, this year it was discovered that Medicare patient details were up for sale on the 'darknet.'

Recognising the vulnerability of digital systems to cyber security risks and interferences with individuals' privacy, the ADHA established the Digital Health Cyber Security Centre to ensure the protection of the national digital health system and Australians' personal health information from cyber threats.

From February 2018, a mandatory data breach notification scheme will be operational in Australia. While this scheme may give Australians greater confidence in the privacy of their MyHR, and greater ability to take action if their MyHR is breached, it places an additional regulatory burden on government agencies and private organisations.

Legal restrictions on the handling of health information

There are several pieces of legislation that restrict the matching and analysis of eHealth data. This legislation may potentially restrict the strategic outcomes proffered by the Strategy. Two such examples are the Privacy Act 1988 (Cth) ('Privacy Act') and restrictions in the My Health Records Act itself.

In Australia, the Privacy Act regulates the handling of personal information (in essence, information that allows an individual to be personally identified). Under the Privacy Act, sensitive information, which includes health information, receives extra protections regarding its collection and handling.

Further, while the Privacy Act generally does not apply to small businesses, all organisations that provide a health service and hold health information (other than in an employee record in private

sector organisations) must comply with the Privacy Act, regardless of their size.

The My Health Records Act contains additional provisions around the handling of health information, and a breach of the My Health Records Act in relation to health information is an interference with privacy for the purposes of the Privacy Act. This means that the Australian Information Commissioner, who enforces the Privacy Act, can take measures in response to such breaches. The My Health Records Act also contains civil and criminal penalties that aim to protect the sensitive information contained in MyHRs and appease concerns associated with storage of health information on an electronic database.

Compliance with these laws can be a significant burden for healthcare providers and researchers looking to leverage the data, which may become available from Australia's move to a digital eHealth system. De-identification of information is often relied upon to overcome this burden. However, in order for de-identification to be successful, re-identification must be incredibly difficult, if not impossible.

For example, in September 2016, researchers alerted the Federal Government that they were able to re-identify de-identified information in a dataset published by the Department of Health. Relying on de-identification may be even riskier in the future as there is a bill before the Commonwealth Senate that would make it a criminal offence under the Privacy Act to re-identify government datasets or publish or communicate such de-identified datasets.

Conclusion

The Strategy and MyHR are set to modernise the management of health records in Australia. By providing a consolidated record of a patient's healthcare history, MyHR will allow healthcare providers to operate with greater efficiency and will ensure patients are provided with higher quality healthcare. However, there are risks to the overall success of the Strategy, and these need to be carefully managed with appropriate governance structures having regard to the regulatory compliance regimes noted above.

Mauritius introduces Data Protection Bill to Assembly

Data Protection Leader confirmed, on 5 December 2017, with Ammar Oozeer, Barrister at BLC Robert & Associates, that the Cabinet of Ministers ('the Cabinet') had agreed, on 1 December 2017, to introduce the Data Protection Bill (No. XIX of 2017) ('the Bill') to the National Assembly. The Bill seeks to bring Mauritius' data protection framework into line with international standards, namely the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), by repealing the Data Protection Act 2004. Additionally, the Bill aims to simplify the regulatory environment for business in the digital economy and promote the safe transfer of personal data to and from foreign jurisdictions.

Oozeer said, "With the expanded territorial reach of the GDPR, the proposed new data protection regime will surely help to spur growth in the Mauritian ICT/business process outsourcing sector, and generally, facilitate the transfer of personal data from EU-based companies to Mauritian companies. With the new regime, it is expected that the country will attract more business opportunities from EU-based companies in emerging areas such as analytics, Big Data and FinTech. By establishing a regime that will provide a level of data protection equivalent to that ensured within the EU, Mauritius should, in principle, be recognised by the European Commission as a third country that provides an adequate level of protection for the purposes of the GDPR."

High Court issues judgement in Morrisons' class action

The Honourable Justice of the High Court of Justice's ('the High Court') Queen's Bench Division, Brian Langstaff, issued, on 1 December 2017, his decision in relation to the class action in *Various Claimants v. Wm Morrisons Supermarket PLC*, addressing whether Morrisons could be held liable for the criminal actions of Andrew Skelton, who maliciously disclosed personal data of co-employees. The High Court determined that although the Data Protection Act 1998 would not impose primary liability on Morrisons, vicarious liability could be established, i.e. the liability for which employers, without personal fault, are held responsible for the wrongs committed by their employees.

David Lorimer, Associate at Fieldfisher LLP, said, "What is interesting about this case is that it emphasises that cyber risks don't just come from external hackers, but can also come from internal, trusted employees. It is the first time a court has held that employers will be vicariously liable for breaches of data protection laws by rogue employees."

The High Court held that primary liability could not be established since Morrisons did not directly misuse any personal data, nor authorise or permit its misuse by any carelessness on its part. However, the High Court justified Morrisons' vicarious liability on the basis of the principle of social justice under common law, finding there was a "sufficient connection between the position in which Skelton was employed and his wrongful conduct, put in the position of handling and disclosing the data as he was by Morrisons" and rejecting the argument that the Data Protection Act, by its terms, would exclude such liability.

DATA PROTECTION LEADER

More publications from Cecile Park Media

Save up to 30% with print and digital edition bundles

Buy 2 Cecile Park Media titles and save 10%

Buy 4 Cecile Park Media titles and save 15%

Buy 6 Cecile Park Media titles and save 20%

Buy all 8 Cecile Park Media titles and save 30%

For subscriptions call us now on +44 (0)20 7012 1387
or visit cecileparkmedia.com

Each of the publications are individually priced, so please contact us for specific information on pricing. We offer four subscription types: single-user, site licence, academic and corporate, all of which can be tailored to your specific needs and come with hard-copy and online access.

Data Protection Leader is published monthly by Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND

Telephone +44 (0)20 7012 1380 Website cecileparkmedia.com

CPM CECILE PARK MEDIA