ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Turkey welcomes the long awaited Data Protection Law

The Law introduces an obligation to register and fines up to €300,000. **Begüm Yavuzdoğan Okumuş** examines Turkey's new data protection law.

For many years, Turkey has lacked separate legislation on the issue of data protection. Previous draft laws that have been sent to the Turkish Parliament were either returned to the proposing committee or not even discussed before the Grand Assembly as Parliament was being dissolved before a general election. However, following the recent general election in November 2015, the current government announced that a Turkish data protection law was high on their

Continued on p.3

Privacy enforcement begins in Singapore: Fines for lax security

New guidelines make it clear that businesses need to pay close attention to compliance. Also Malaysia takes steps in showing stronger enforcement. By **Graham Greenleaf**.

Singapore's Personal Data Protection Commission (PDPC) has published nine data protection enforcement decisions, the first since the Personal Data Protection Act 2012 (PDPA) came into force in July 2014.[1] At the same time, it has issued advisory guidelines on enforcement. This article outlines these developments and their significance in the context of Singapore's legislation. Increased emphasis on

Continued on p.4

Issue 141 **June 2016**

INTERNATIONAL report

ISSUE NO 141 **JUNE 2016**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

SUB EDITOR
Tom Cooper

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

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

CONTRIBUTORS
Begüm Yavuzdoğan Okumuş
Gun+Partners, Turkey

Kuan Hon
Queen Mary University of London, UK

Nick Graham and Jane Bentham
Dentons LLP, UK

Adèle Kendler
PL&B Correspondent

Jiří Maštalka
Office for Personal Data Protection,
The Czech Republic

Irene Kamara and Paul de Hert
Vrije Universiteit, Belgium

Christian Schaefer
Asia Counsel, Vietnam

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International 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 2046-844X

comment

Turkey adopts a law and joins the DP community

Our front page stories reflect the international trend of growing privacy protection – a new DP law in Turkey and stronger enforcement in Singapore. The situation in Turkey is certainly interesting as at the time of the law being adopted, the Turkish citizenship database had been hacked. This security breach potentially risked personal information of some 49 million citizens. It has been alleged that the leak was politically motivated against President Recep Tayyip Erdoğan. Turkey's law is based largely on the EU DP Directive but there are also some novelties (p.1). Organisations with operations in Turkey will now need to review their programmes.

We will hear more about Turkey's law at our summer conference 4-6 July 2016 in Cambridge, and are very fortunate to welcome Dr. Elif Küzeci, Professor of Law, University of Bahçesehir, Turkey.

Since our last issue, the EU DP Regulation (GDPR) has finally been adopted (p.11 and p.17) and this issue includes a detailed analysis of the differences between the old Directive and the new Regulation on international data transfers (p.7). We also report on the new status of biometric data as sensitive data under the GDPR (p.12), and how the UK's business-friendly regulatory environment may have to change as a result of the GDPR (p.17).

Also to be noted is that the European Commission has published the text of Directive 2016/680, which governs data processing in law enforcement situations; and the Passenger Name Record Directive 2016/681 (p.11).

Developments in Asia include extensions of Vietnam's data privacy protections through its new Cybersecurity Law (p.26) and the appointment of a Privacy Commission in the Philippines (p.22). Singapore has started enforcement and issued guidance on aggravating and mitigating factors when considering financial penalties (p.1).

On the management side, we report on why the Netherlands DPA investigated a Nike running app, how the company responded (p.14), and the guidance now available on how to manage privacy aspects of wearables and health apps.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Turkey... from p.1

priorities for their legislative programme and adoption of the same was a real need for Turkey's EU harmonization process. To this effect, a Draft Law on the Protection of Personal Data was submitted to the Grand Assembly on 18 January 2016 and entered into force as of 7 April, 2016.

The Law on Protection of Personal Data ("Law"), which is very much in line with the EU Directive 95/46/EC ("EU Directive"), contains detailed provisions relating to the protection of personal data, an area that was previously only covered by insufficient and piecemeal applications of different legislative measures and the general rules of the Turkish Constitution.

Personal data

The Law introduces an official definition for the term "personal data", defining it as "any type of information that relates to an identified or identifiable natural person". In this sense, the Law provides a definition that is parallel to the EU Directive, though one that is slightly less detailed.

The central principle is that personal data can only be processed once the data subject has provided explicit consent. However, if at least one of the following exceptions exists, personal data can be processed without obtaining explicit consent:

- The processing is clearly mandated by laws,
- It is impossible to obtain the individual's explicit consent, but the processing is required for the safeguarding of their or a third person's life or physical wellbeing,
- The processing is directly related to the formation or execution of an agreement to which the data subject is a party,
- Processing is required for the data controller to satisfy their legal obligation,
- The data to be processed has been made public by the data subject,
- Processing is mandatory for the establishment, use or protection of a right,
- On the condition that it does not harm the data subject's fundamental rights and freedoms, the processing is mandatory for the legitimate interests of the data controller.

Personal data of a special nature

The Law also separately distinguishes a category of "personal data of a special nature" which is subject to a more extensive level of protection. The types of personal data that fall under this category are related to race, ethnicity, political views, philosophical beliefs, religious denomination or other beliefs, clothing and attire, membership of associations, charities or trade unions, health, sex life, convictions, security measures and biometric data.

As in the general category of personal data, the central prerequisite for processing such data is the explicit consent of the data subject. However, in the situation where at least one of the following exceptions exists, there is no longer a requirement for explicit consent:

- Excluding health and sex life data, the processing is clearly mandated by law,
- Regarding sex life and health data, the data is to be processed by persons or authorized institutes bound by the duty of confidentiality for the purpose of the protection of public health, the provision of medical, diagnostic and treatment services and the planning, managements and financing of healthcare services.

By setting an additional level of protection, the Law dictates that personal data that falls under this category can only be processed if a data controller adheres to the appropriate precautions published by the Data Protection Institution, when it is established.

Therefore, the current standard operating procedures regarding data protection in Turkey must be reviewed by each company engaging in such activities – particularly if the scope of processing cannot be said to fall under any of the aforementioned exceptions.

Data Protection Institution under PM

The Law provides, within six months from its enactment, for the incorporation of the Personal Data Protection Institution ("Institution"). The Institution will be positioned under the Prime Minister's office, and will consist of the Data Protection Board ("Board") and a President and shall be primarily responsible for enforcing the Law. Further, a Register of Data Controllers will be established and maintained by the Institution within six months after the enactment of the Law. Data controllers are required to be registered with the Register of Data Controllers before processing personal data. The registration will include, among other details, information on the measures taken for ensuring data security, data which will be transferred to third parties and/or other countries, and the maximum period of retention for processed personal data.

Transfer of data

The Law contains provisions relating to the general transfer of data and the transfer of data abroad. With regard to the general transfer of data, the central principle remains that explicit consent is required. However, the exceptional situations set out above are applicable again for personal data to be transferred without obtaining explicit consent.

For transfer of personal data abroad the explicit consent of the data subject is required. Again however, if the exceptional situations set out above exist, the transfer of the data abroad may only take place if:

- the foreign country has sufficient safeguards or,
- if they do not have such adequate safeguards, the data controller in the foreign country, has applied to the Institution with an undertaking in writing for equivalent safeguards and has obtained the Board's permission.

Countries that have sufficient safeguards are to be determined by the Institution and a list of these countries will be published. Last but not least, as a result of long discussions in the Parliament, the Law includes a provision indicating that personal data can be transferred abroad in cases where the interest of Turkey or the data subject can be adversely affected, provided that the approval of the Institution is obtained, taking into account international treaties.

The primary obligations of the Data Controller

The Law will introduce a host of obligations on data controllers to

ensure that personal data is processed and transferred lawfully and proportionately. The most important of these obligations are the requirements to inform the data subject, and to erase, destroy or anonymize personal data that is outside the purpose of its purpose of processing.

The data controller's obligation to inform the data subject should especially be taken into account while drafting the consent forms and agreements that are to be presented to the data subject. The scope of this obligation covers providing information on the identity of the data controller, the purposes of data processing and data transfer, the legal justification behind the data collection, methods of collection of personal data, and the rights of the data subject. These are granted by the Law in relation to the right to request information on whether personal data is being processed or not, whether data is being transferred to third parties and details on those third parties and the purpose of the data controller in processing personal data. Data subjects also may request compensation for damages they have suffered due to unlawful processing of their personal data and to object to the conclusions that are to their detriment and that are reached through the process of personal data by automated means.

Data Controllers must ensure data security

The Law further introduces data security obligations for data controllers and stipulates that data controllers are under an obligation to implement all kinds of technical and administrative measures to maintain a security level that would avoid unlawful processing of and access to personal data, whilst also safeguarding personal data. The Law clearly regulates that the data controller and the subcontractor and/or the data processor that process data on behalf of the data controller are jointly liable for maintaining the security measures. This provision requires careful drafting of the recourse provisions under the subcontractor agreements between data controllers and data processors. The reason is that both parties will be jointly liable to the data subject whereas the data controller would most probably want the subcontractor to assume full liability for data security.

It should also be noted that the data controller has a duty to inform the Board and the relevant party if and when personal data has been unlawfully accessed. Thereafter, the Board has the discretion to announce the breach on its website or via another communications channel.

Administrative sanctions

In addition to criminal sanctions stipulated under the Turkish Criminal Code and repeated under the Law once again, the Law introduces administrative sanctions.

As per Article 18 of the Law, data controllers may face administrative monetary sanctions between the range of 5,000 Turkish Lira (approximately €1,500) and TRY 1,000,000 (approximately €300,000). Sanctions are specifically regulated for data controllers that are in breach of their obligations to inform the data subject, ensure data security, enforce the decisions of the Board and to register with the Register of Data Controllers.

These sanctions shall enter into force after six months from the enactment of the Law. The important matter here is that the current provisions of the Turkish Criminal Code imposing criminal sanctions will be also be suspended for a period of six months after the enactment of the Law.

Transition period

Under the Law, there is a transition period for two years meaning that personal data that has been processed prior to the enactment of the Law must be brought into compliance with its provisions within this period. In cases where such compliance is not achieved, non-compliant personal data shall be deleted, destroyed or anonymized. However, personal data for which consent from data subjects was obtained legitimately before the enactment of the Law will be held compliant with the Law, unless a contrary statement is obtained from the data subject within a year.

It is currently not clear how companies can adapt themselves to the Law and ensure all personal data obtained will be brought into compliance, or how personal data will be deleted, destroyed or anonymized. Secondary regulations will be prepared within a year of the law's enactment. It is expected that guidelines will also be prepared by the Institution to shed light on ambiguous areas.

AUTHOR

Begüm Yavuzdoğan Okumuş is Managing Associate at of Istanbul-based law firm Gun+Partners.
Email: begum.yavuzdogan@gun.av.tr

Singapore... from p.1

enforcement in Asian countries can also be seen in a Malaysian initiative outlined here and in the appointment of the Philippines National Privacy Commission (see p. 22).

Security failures lead to fines

Fines of S$50,000 were ordered against K Box Entertainment Group and S$10000 against its data intermediary, Finantech Holdings, in the PDPC's most significant decision.[2] Because of inadequate security, sensitive data which could facilitate identity theft had been disclosed on about 317,000 K Box members. The relevant test in the PDPA is whether a data controller has implemented "reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks" (s. 24). The PDPC identified numerous ways in which K Box failed to meet that standard, including: it failed to enforce its own password policy, thereby permitting the use of weak passwords; it had weak control over unused accounts by failing to delete them; and it "failed to utilise newer versions of the software library and/or to conduct audits of the security of its database and system". Any of these failures, the PDPC found, could have resulted in vulnerabilities

through which data was disclosed. It was not necessary for the PDPC to identify which security failing had in fact resulted in the disclosures, because these failings were in themselves breaches of the Act. K Box was also issued directions and penalised for the absence of a Data Protection Officer, a breach of its "openness" obligations under the Act (s. 11).

The PDPC found that Finantech, which "had been involved in the setting up and day-to-day processing of K Box's personal databases from 2007," was a data intermediary of K Box. Therefore K Box had the same obligations in respect of the personal data processed on its behalf and for its purpose by Finantech as if the personal data were processed by K Box itself (s. 4(3)). Finantech had failed to meet its security obligations under section 24 because it had failed to put in place the required security measures that K Box needed in order to provide adequate protection for K Box's data and systems. It had not taken any steps to advise K Box of its need to put in place adequate security measures. The PDPC has therefore been very thorough in allocating responsibility for breaches in all ways that the Act allows this to be done.

Other fines and warnings

The Institution of Engineers, Singapore, had imposed on it a financial penalty of S$10,000 (plus directions issued to it) for failing to secure its IT system, resulting in unauthorised disclosure of the personal data of more than 4,000 of its members.[3] Another unauthorised disclosure of personal data on over 900 customers by Fei Fah Medical Manufacturing resulted in a S$5,000 fine.[4]

The other six decisions reported did not result in fines, but only in directions or warnings being given. All but two involved respondents who failed to make reasonable security arrangements. These included failures to prevent unauthorised disclosure of personal data while sending out emails to some 165,000 members; of unauthorised disclosure of personal data on computers at a furniture fair, which collected the data for a lucky draw; and of unauthorised access to personal data held in Metro's IT systems. Even the Singapore Computer Society received a warning for failing to put in place reasonable security measures to prevent the accidental disclosure of the personal data of 214 registrants of an event via email.

The two complaints which did not involve security failures resulted in a warning to a tuition agency for disclosing tutors' personal data on its website without consent, and a warning for disclosing a passenger list, with 37 customers' personal data, to other customers without consent.

Enforcement Guidelines

The PDPC's Advisory Guidelines on Enforcement of Data Protection Provisions[5] are non-binding, but failure to observe them may prove costly for businesses in Singapore. The guidelines on alternative dispute resolution make it clear that the PDPC will take an interventionist role to ensure that parties resolve disputes, including referring complaints back to respondents but monitoring their resolution efforts, facilitating settlements, referring complaints for mediation, and directing other forms of complaint resolution (Part II). There are quite detailed guidelines on how the PDPC will exercise its power to review decisions about failure to provide access, access fees, or failure to provide corrections (Part III). Guidelines on investigation of complaints make it clear that the PDPC has considered many aspects of its considerable investigative powers (Part IV). Where the PDPC gives directions to respondents to secure their compliance, those directions may be quite broad, including steps to nullify the effect of breaches (e.g. non-use of improperly collected data), to reduce harm or future harm, and to change the practices of respondents to prevent future breaches (Part V).

Perhaps the most important reading for businesses are the lists of Aggravating Factors and Mitigating Factors that the PDPC will take into account when considering financial penalties (up to S$1M). These include the extent of active and prompt resolution with customers; taking reasonable steps to prevent breaches occurring (particularly where large quantities of data or sensitive data are concerned); voluntary offers of remedies; immediate notification to individuals, and to the PDPC, when breaches occur; and cooperation with the PDPC in investigations.

> PDPC will take an interventionist role to ensure that parties resolve disputes

Good citation practice

Singapore's PDPC is making its decisions easy to cite (and therefore more likely to be of future influence), by adopting the "neutral citation" standard that is adopted by Singapore's Courts, by DPAs in Hong Kong, New Zealand and Australia (as recommended by the Asia-Pacific Privacy Authorities[6]), and as adopted by a large proportion of courts in the common law world. For example, the citation for the first decision PDPC issued this year is "[2016] SGPDPC 1", and if 15 decisions are issued next year, the citation of the last of those will be "[2017] SGPDPC 15." This is a good step toward transparency of their work.

Malaysia makes enforcement easier

In contrast with Singapore, Malaysia's Department of Personal Data Protection[7] has not yet shown any visible signs of enforcing its Personal Data Protection Act 2010 (PDPA), despite that Act being fully in force for over two years. One reason is that, in effect, the Malaysian PDPA can only be enforced through prosecutions, and those must be with the consent of the Public Prosecutor. The Commissioner cannot even issue an enforcement notice if a breach is not likely to be repeated (the same crippling deficiency as Hong Kong's law had before its 2012 reforms).[8]

However, Malaysia has a new

regulation in force which allows the Commissioner under the PDPA[9] to offer to compound specified offences under the Act. In other words, if the Commissioner so offers (again with the consent of the Public Prosecutor), this allows a party alleged to have committed an offence to pay what is in effect a fine prior to a prosecution being commenced. The Commissioner chooses the amount for which the offence may be compounded, up to 50% of the maximum fine for the offence (PDPA, s. 132). If the "fine" is paid, prosecution cannot proceed. The compoundable offences in Schedule 1 include "Contravention of the data protection principles", the most general offence in the Act, and various other important provisions concerning corrections, requests to cease processing, sensitive data, and direct marketing.

Local lawyers consider that "[t]he Regulations will ease the backlog of prosecution cases and may signal the start of stronger enforcement of the PDPA".[10] Such forecasts will only be fulfilled if the Commissioner also publicises cases which have been compounded, and the amounts involved, so that the 'tariff' for particular offences becomes known.

Conclusions

Although it is a modest beginning, Singapore is leading the way among ASEAN countries with enforcement of data privacy laws. It already has strong enforcement of the Do-Not-Call (DNC) aspect of its law. The advisory Guidelines on enforcement make it clear that if businesses wish to avoid significant fines or other sanctions, pro-active responses to privacy problems when they are first discovered will have a significant effect.

REFERENCES

1 PDPC Data Protection Enforcement Cases (to 21 April 2016) www.pdpc.gov.sg/commissions-decisions/data-protection-enforcement-cases
2 Breach of Protection and Openness Obligations by K Box Entertainment Group and Finantech Holdings [2016] SGPDPC 1.
3 Breach of Protection Obligation by Institution of Engineers, Singapore [2016] SGPDPC 2.
4 Breach of Protection Obligation by Fei Fah Medical Manufacturing [2016] SGPDPC 3.
5 PDPC Advisory Guidelines on Enforcement of Data Protection Provisions 21 April 2016 www.pdpc.gov.sg/docs/default-source/advisory-guidelines-on-enforcement/advisory-guidelines-on-enforcement-of-dp-provisions-(210416).pdf
6 Asia-Pacific Privacy Authorities Common administrative practices – Case Note Citation www.appaforum.org/resources/common_practice.html#citation
7 Department of Personal Data Protection (Malaysia) website www.pdp.gov.my/index.php/en/
8 For details of enforcement of Malaysia's PDPA, see G. Greenleaf Asian Data Privacy Laws: Trade and Human Rights Perspectives (OUP, 2014), pp.332-335.
9 Personal Data Protection (Compounding of Offences) Regulation 2016 (Malaysia), in force 16 March 2014.
10 Wong & Partners Client Alert April 2016.

Ireland to challenge model clauses as basis for international transfers

Ireland's Data Protection Commissioner is planning to refer the Facebook case back to the Court of Justice of the European Union (CJEU) to determine if Facebook can continue to transfer data from the EU to the US by using EU model clauses, Max Schrems' website Europe v Facebook has announced.

"In an unpublished draft decision of May 24th 2016 the Irish DPC followed the objections of the Complainant Mr Schrems in the procedure between Mr Schrems and Facebook Ireland Ltd. Mr Schrems claimed that Facebook USA continues to be subject to US mass surveillance laws, independent of the use of "model causes" or "Safe Harbor" and that his data continues to be subject to fundamental rights violations once it reaches the United States.'

Max Schrems said: "This is a very serious issue for the US tech industry and EU-US data flows. As long as far-reaching US surveillance laws apply to them, any legal basis will be subject to invalidation or limitations under EU fundamental right[s]. I see no way that the CJEU can say that model contracts are valid if they killed Safe Harbor based on the existence of these US surveillance laws. All data protection lawyers knew that model contracts were a shaky thing, but it was so far the easiest and quickest solution they came up with. As long as the US does not substantially change its laws I don't see [how] there could be a solution.'

These developments could further complicate international data transfers. As we wait for the approval of the EU-US Privacy Shield framework, companies have been told that they can in the meantime rely on EU model clauses and Binding Corporate Rules.

• *For further details see www.europe-v-facebook.org/PA_MCs.pdf*

• ***Great Expectations**, PL&B's 29th Annual International Conference 4-6 July in Cambridge has a session entitled 'The EU-US Privacy Shield and the future of EU adequacy for 3rd countries'. Speaker: Bruno Gencarelli, Head of the Data Protection Unit, Justice, European Commission.*
See www.privacylaws.com/ac29 for the full programme and session summaries.

International transfers under GDPR: Key changes

Organisations that currently rely on model clauses should start working to replace them with GDPR model clauses as soon as their form becomes available, **Kuan Hon** says.

The General Data Protection Regulation[1] (GDPR) is finally law, becoming directly effective to replace the 1995 EU Data Protection Directive (DPD) in all EU Member States from 25 May 2018, without requiring national implementing legislation[2]. Like the DPD, it applies across the European Economic Area (EEA). GDPR enhances the role of the European Data Protection Board (Board), which will replace the working party of national Data Protection Authorities (DPAs) formed under Art. 29 DPD (WP29).

With a few exceptions, GDPR Chapter V Arts. 44-50 generally tightens up rules on international transfers (i.e. transfers "to" third countries outside the European Economic Area), currently governed by DPD Arts. 25-26. This article summarises the main changes, discusses practical implications (including for cloud computing), and highlights unresolved policy issues.

Current position

Under Arts. 25-26 DPD, "transfers" of personal data "to" third countries (outside the European Economic Area) are prohibited unless:

- There is "adequate protection", such as through a European Commission Decision "whitelisting" the third country in question;
- "Adequate safeguards" are provided, such as through transferees signing contracts in a form previously approved by Commission Decisions ("standard contractual clauses", often called "model clauses"), or through "binding corporate rules" (BCRs) entered into by members of a corporate group and authorised by relevant DPAs to permit transfers between such members; or
- A derogation can be used, such as data subject consent, or necessity for the performance/conclusion of certain contracts.

GDPR preserves this basic hierarchy (although changing "adequate safeguards" to "appropriate safeguards"), with some important differences.

Key changes

The table below summarises some key changes.

KEY DIFFERENCES BETWEEN THE EU DP DIRECTIVE AND GENERAL DATA PROTECTION REGULATION

DPD	GDPR
Application of transfer restriction	
Art. 25: - Controllers only - Transfer to third country - Initial "transfer"	Art. 44: - Controllers **and processors** - Transfer to third country **or international organisation** - Initial transfer **and any "onward transfer"**
Adequate protection	
Under Art. 25(2) some EU Member States, e.g. the UK, allow controllers to self-assess adequacy of protection in the context of individual circumstances	**No more self-assessment** – only the Commission, after consulting the Board (Rec. 105), decides[3] on the adequacy (or inadequacy) of a third country (or specified sector), territory or international organisation, subject to approval by a committee under Art. 93(2)[4] - Art. 45
Art. 25(2) lists factors to consider when assessing adequacy of protection	Factors the Commission must consider are expanded, largely based on WP29 opinions,[5] but also including whether "essentially equivalent" protection is ensured (Rec. 104),[6] and public authorities' access to data - Art. 45(2)
	Note: Commission "whitelisting" Decisions under the DPD remain valid until amended/replaced/revoked under the GDPR -Art. 45(9)
	The Commission must review GDPR and DPD adequacy Decisions at least every 4 years (Art. 45(3), Rec. 106, Art. 97(2)(a)), publicising its report (Art. 97(1)), and monitor developments affecting such Decisions (Art. 45(4)).

KEY DIFFERENCES BETWEEN THE EU DP DIRECTIVE AND GENERAL DATA PROTECTION REGULATION	
DPD	**GDPR**
Safeguards	
Art. 26 - without adequate protection, transfers are permitted under "adequate safeguards", including:	Art. 46 - without adequate protection, transfers are permitted under **"appropriate" safeguards**, if enforceable rights and effective legal remedies for data subjects are "available". Such safeguards may be provided, "without needing specific DPA authorisation", in several listed ways, including:
BCRs - not envisaged by the DPD, but developed by organisations with DPAs and authorised by DPAs under Art. 26(2)	**BCRs** – BCRs meeting Art. 47's requirements must be approved by the competent DPA, applying the new consistency mechanism.[7]
Commission-approved standard contractual clauses (aka model clauses) under Art. 26(4) – 3 sets, currently	**Standard contractual clauses** - Commission-adopted[8]
	New: **standard contractual clauses - DPA-adopted**, if Commission-approved[9]
DPAs may authorise transfers under Art. 26(2) including individual instruments, *ad hoc* contracts, administrative arrangements	New: **legally-binding instrument** between **public authorities**
	DPA authorisation under **consistency mechanism**: - **Contractual clauses** (i.e. *ad hoc* contracts) - Provisions in **administrative arrangements** between public authorities which include enforceable and effective data subject rights
	New: GDPR-approved codes of conduct or certifications "together with binding and enforceable commitments" of the third country controller or processor to apply the safeguards including as regards data subject rights (also Art. 41(2))
	Note: model clauses Decisions and DPA authorisations under DPD remain valid, so transfers under DPD model clauses, existing BCRs or DPA-authorised intra-group agreements etc. are permissible until the relevant DPD Decision or authorisation is amended/replaced/revoked under the GDPR - Art. 46(5)
Derogations	
Art. 26(1) - without adequate protection/safeguards, transfers are permitted under a derogation, including:	Art. 49 - without adequate protection or appropriate safeguards, transfers are permitted under a derogation, including:[10]
Data subject's unambiguous consent to the proposed transfer	Data subject's **explicit** consent, **having been informed** of the possible risks for the data subject due to the absence of an adequacy decision and appropriate safeguards
Transfer necessary or legally required on important public interest grounds	Transfers necessary for important reasons of public interest (only interests **recognised by EU law** or the controller's national law). The so-called "anti-FISA" provision, Art. 48, specifically prohibits transfer/disclosure under any third country judgment/decision unless based on international agreement, e.g. a mutual legal assistance treaty (MLAT)[11]
	New: Absent adequate protection, appropriate safeguards or a derogation – transfers may be made if necessary for the controller's compelling legitimate interests; very limited scope; prescriptive conditions/requirements (Art. 49(1), (6))

KEY DIFFERENCES BETWEEN THE EU DP DIRECTIVE AND GENERAL DATA PROTECTION REGULATION
Other issues where GDPR differs from DPD
National limitations - for countries/territories/sectors where no Commission adequacy Decision has been issued, EU or Member State law may, "for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data" and notify them to the Commission (Art. 49(5))
Mandatory notifications to data subjects must include information on proposed transfers, adequacy Decisions or safeguards and the **means to obtain a copy** (Arts. 13(1)(f), 14(1)(f), 15(2))
Controller-processor contracts must include provisions restricting transfers – Art. 28(3)(a)
Controller and processor records must include certain information on transfers – Arts. 30(1)(e), 30(2)(c)
Member States must provide **exemptions/derogations** from the transfer restriction if necessary to balance data protection with **freedom of expression** (Art. 85(2)). They may also provide specific safeguards regarding transfers in the **employment context** (Art. 88(2))
International agreements between the EU and third countries may allow transfers with appropriate safeguards; new agreements must not "affect" GDPR and must include "appropriate" protection (Art. 96, Rec. 102)
International cooperation by DPAs with third countries is encouraged, for enforcement, mutual assistance etc. (Art. 50)

Practical implications

Both controllers and (for the first time) processors will be exposed to huge administrative fines (€20 million or 4% total annual turnover if higher) for infringing the GDPR's transfer restrictions, or non-compliance with DPA orders to suspend transfers (Arts. 83(5), 58(2)(j)). This means that managing compliance with the transfer regime will be more important than ever. Processors will need to get to grips with all their GDPR obligations, but the transfer regime is particularly significant because, while lower-tier fines apply to infringements of most processor obligations, higher-tier fines apply to transfers.[12]

Organisations relying on self-assessment of adequacy (e.g., based on strong encryption pre-transfer) will need to find other transfer methods.

The continuing validity of existing Commission Decisions (whitelisted countries, model clauses) and BCRs authorised under the DPD will afford organisations some breathing space. However, Commission Decisions under the DPD (and indeed GDPR) remain vulnerable to challenge before the CJEU, e.g. by DPAs:[13] not only model clauses Decisions, but also any adequacy Decision on the EU-US Privacy Shield proposed to replace the now-invalid Safe Harbour Decision.[14]

Future Commission Decisions adopting GDPR model clauses are likely to contain provisions revoking the equivalent DPD model clauses Decisions, but hopefully they will provide for a reasonable transitional period before such revocation takes effect, because organisations will need time to replace their existing model clauses contracts – in some cases, possibly thousands of contracts - with the new GDPR model clauses. The International Chamber of Commerce was instrumental in advocating workable model clauses under the DPD, and hopefully industry bodies will expedite discussions with the Commission on feasible GDPR-compliant model clauses. Organisations that currently rely on DPD model clauses should of course start working to replace them with GDPR model clauses as soon as their form becomes available, or consider alternative transfer methods.

> Hopefully industry bodies will expedite discussions with the Commission on feasible GDPR-compliant model clauses.

Member States should no longer be able to require specific DPA authorisation for GDPR model clauses or BCRs authorised by the competent DPA, which will benefit organisations. BCRs may therefore become more feasible. However, because the consistency mechanism[15] applies to BCR authorisations, the process may still be time-consuming and expensive, and therefore remain unaffordable for many. BCRs may allow transfers not only within the same corporate group, but also within a "group of enterprises engaged in a joint economic activity". Given BCRs' time/costs, it seems unlikely that unaffiliated enterprises would consider BCRs except for substantial medium/long-term "partnerships" or joint ventures. Processor BCRs will no longer be possible unless the group has an EU-established member (unlike currently, when the non-EU headquarters can assume liability).

New "appropriate safeguards" increase the range of transfer methods available. Standard contractual clauses promulgated by DPAs may be used, once approved by the Commission. Promisingly, transfers will be permissible to recipients adhering to GDPR-approved codes of conduct or certifications (with binding commitments to

apply the safeguards[16]). Again, industry bodies could put forward for approval sector-specific codes/certifications, such as for cloud computing, and seek clarification regarding the "binding commitments" that will be required. The competent DPA may authorise *ad hoc* contractual clauses under the consistency mechanism. Public sector organisations may make transfers to non-EU public authorities under legally-binding instruments without specific authorisation, or (if authorised by the competent DPA under the consistency mechanism) through provisions in administrative arrangements which include enforceable data subject rights. As applying the consistency mechanism is likely to increase delays and costs (and may even result in some authorisations being declined), organisations might wish to avoid transfer methods that require it, where possible.

For derogations, transfers relying on consent will require care, given the requirement for explicit consent after notification of the risks. A proposed "legitimate interests" derogation will rarely be usable because, as enacted (a replacement of sorts for DPD self-assessment, with circumstances/context being considered), it is very narrow and prescriptive.

Despite the GDPR's avowed aim of harmonising data protection laws across the EEA, organisations must still monitor applicable local laws for any specific national limitations, exemptions/derogations for freedom of expression, or additional safeguards in the employment context. Further information/guidelines are also expected from the Commission and the Board, such as forms of GDPR model clauses, detailed conditions for approving codes/certifications, what codes/certifications will be approved, etc. It is hoped that they will address various uncertainties and inconsistencies regarding the transfer restriction.[17]

Cloud computing

When controllers use cloud computing to process personal data, the position varies with service type.

With IaaS/PaaS, often customers can choose the "region" or even country where they wish their data to be processed, such as EU, or Germany. Cloud providers are increasingly building data centres in the EU, and GDPR's imposition of transfer restrictions on processors (including cloud providers) would further incentivise this. For their own protection, non-EU providers generally reserve rights to move data from the customer's selected region if required by law, but if the relevant law is non-EU, e.g. US, GDPR prohibits this, putting them in the invidious position of having to decide which law to break.[18]

Selecting an EU region will not necessarily prevent storage in third countries of some metadata (e.g. account information) and/or back-ups/failover etc, or prevent remote access to EU personal data by third country support personnel.[19] Many non-EU providers offer DPD model clauses to business customers, although usually only on an opt-in basis, which customers should activate for caution's sake. Presumably those providers will offer GDPR model clauses once available. US-based providers might also sign up to the proposed Privacy Shield[20] if approved.

With many SaaS services, customers cannot control data processing locations, although some allow business customers to select regions. Perhaps more SaaS providers will start enabling region choice for their business customers. But again, many non-EU SaaS providers offer model clauses, and customers will be requesting GDPR-compliant model clauses (or the Privacy Shield) in time. With "layered" cloud, e.g. SaaS built on IaaS/PaaS, GDPR's Art. 28 contract requirements may prove more problematic than the transfer restriction.[21]

Whatever the type of cloud service, providers may consider adhering to GDPR-approved codes of conduct or certifications to legitimise customers' transfers to them, when more information is known about such approvals and the required accompanying commitments. Developing such transfer methods seems worthwhile, although it is unknown whether smaller providers could afford such codes/certifications.

Policy issues

Data export rules, generally interpreted[22] as rigidly restricting physical location of data to certain regions or countries, are problematic. A book based on my PhD thesis, forthcoming from Edward Elgar, will illustrate these problems by reference to transfer restrictions in cloud computing.

Data localisation requirements are often driven by emotion and politics rather than technology, law or even logic, flying in the face of increasing globalisation, even threatening to reverse it. What would happen if all countries parochially trust only their "own" laws (even when non-EU countries are increasingly adopting DPD-like laws), and refuse to allow organisations to obey applicable laws of other countries where they operate? Given that many non-EU organisations will be directly subject to GDPR (not just to "equivalent" laws),[23] why should transfers to them be restricted? The fundamental underlying issues that need resolution relate not to data location *per se*, but cross-border enforcement, and conflicts between laws of different jurisdictions when organisations operate multinationally.

Data localisation laws suffer from other fundamental flaws. Adequate data protection ultimately relies not on laws but on actions taken by transferors/transferees. It is misconceived to assume that only laws, and not technical measures such as encryption, can protect data, and to discount or undervalue such measures when in fact laws should incentivise them. Knee-jerk reactions to other countries' surveillance/mass collection of personal data,

Issues that need resolution relate not to data location *per se*, but cross-border enforcement, and conflicts between laws.

when EU DPAs have no supervisory control over similar surveillance/collection by EU intelligence agencies, divert attention from the need for the EU to put its own house in order[24]. And if data protection laws' aim is to protect privacy, regulation should be based on control of logical access to intelligible data, regardless of physical location. The fixation on restricting data location again allows encryption to be disregarded or devalued.

Transfer restrictions under the DPD and GDPR, as currently interpreted, hugely increase bureaucracy (and legal fees) without necessarily improving privacy protections for citizens. It is hoped that the Board, industry bodies and business organisations will strive to provide the leadership needed to make GDPR transfers workable in the modern digital world.

AUTHOR

Dr. Kuan Hon www.kuan0.com is a consultant lawyer for Pinsent Masons and senior researcher with Queen Mary University of London, but this article is written purely in her personal capacity and should not be taken to represent the views of any organisation with which she may be associated.

REFERENCES

1 Regulation (EU) 2016/679 http://tinyurl.com/gnp24vo
2 Although Member States will have to address any conflicting national laws.
3 Commission adequacy Decisions are challengeable (Schrems ECLI:EU:C:2015:650 http://curia.europa.eu/juris/documents.jsf?num=c-362/14 invalidated the Safe Harbor Decision allowing transfers to certain US organisations), e.g. for undermining DPAs' independence or allowing transfers to countries with excessive surveillance (see further WP237 http://tinyurl.com/hkpvudr).
4 Many Commission proposals, e.g. for whitelisting third countries, adopting GDPR model clauses, approving DPA-adopted model clauses, require approval by this Article 93(2) committee. A list plus flowchart explaining the process and stages is at http://blog.kuan0.com/2016/05/article-932-gdpr-comitology-flowchart.html.
5 Notably WP12 http://tinyurl.com/hy9v35y
6 Based on Schrems, n. 3.
7 To ensure consistent cross-EU application of the GDPR, involving the Board, with procedures for decision, dispute resolution if DPAs disagree, etc. - details are out of scope.
8 See n. 4.
9 See n. 4.
10 Space does not permit discussion of changes regarding transfers for legal claims, to protect the vital interests of the data subject or others, or from public registers.
11 The UK considers it is entitled not to opt in to this provision, and will not do so - http://tinyurl.com/zgecmhw and http://tinyurl.com/hmf2wvc - although exactly which parts it will not opt in to remain unclear. See also *PL&B UK* March 2016, p.1.
12 Arts. 83(4)-(5) GDPR stipulate two tiers of administrative fines for infringement of GDPR obligations - €20 million or 4% total annual turnover if higher, for obligations considered key; and €10 million or 2% total annual turnover if higher, for other obligations.
13 N. 3.
14 http://europa.eu/rapid/press-release_IP-16-433_en.htm
15 N. 7.
16 Insisting on legally-binding commitments from recipients for all "appropriate safeguards" is inflexible and retrogade. It fails to recognise that in some situations, e.g. strongly-encrypted data where recipients cannot access decryption keys, code can protect data as well as – or better than - contract. See/www.scl.org/site.aspx?i=ed35439.
17 Including: can Member States limit transfers of specific categories to countries whitelisted under DPD adequacy Decisions, but not GDPR adequacy Decision yet? Exactly what binding commitments are required to validate Art. 46 "appropriate safeguards"? How can onward transfers be legitimised in practice (indeed what are considered "onward transfers"? – Rec. 101 cf. Art. 44)? Are transfers necessary for the performance/conclusion of certain contracts permitted even when more than "occasional" (Rec. 111)? Precisely what can data subjects request a "copy" of under Arts. 13(1)(f), 14(1)(f)?
18 Except perhaps with data located in the UK! – n. 11. The UK's "non-opt-in" seems set to spark disagreements about its right to do so, and concerns about circumventing Art. 48 by transmitting personal data to the UK first.
19 Remote access by third country persons to personal data physically located in the EEA is generally considered to constitute "transfer".
20 N. 14,
21 See www.scl.org/site.aspx?i=ed46375
22 Unfortunately "transfer" remains undefined, although the European Data Protection Supervisor suggested a definition - http://tinyurl.com/ozywy5p
23 See *PL&B International* April 2016, pp.25-28.
24 http://preview.tinyurl.com/hkpvudr

EU DP Regulation in force 25 May 2018: Time to start preparing for compliance

The EU Data Protection Regulation entered into force on 24 May 2016 and this will be applied from 25 May 2018.

Together with EU Regulation 2016/679, the European Commission has published the text of the so-called Police Directive, which is available at http://tinyurl.com/hgaz9vu, and the Passenger Name Record Directive (http://tinyurl.com/gwqxc67).

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

• *The text of the Regulation – in all languages – is available at http://tinyurl.com/gnp24vo*

• *Businesses now have two years to start their preparation process. Join the main players with 40+ speakers from 16 countries at* ***Great Expectations****, PL&B's 29th Annual International Conference, 4-6 July at St. John's College, Cambridge to learn how to work towards compliance. The full conference programme is on the PL&B website at www.privacylaws.com/ac29*

Top 10 tips for processing biometric data

Biometric data is defined as sensitive under the GDPR. **Nick Graham** and **Jane Bentham** discuss the implications.

Biometric data use is undergoing a major shift. From having been the sole domain of law enforcement and government agencies (think national security and border control, police investigations and so on), we are now seeing an increase in use across a spectrum of commercial sectors, including retail, social media, finance, manufacturing, telecoms, and general business. Biometrics is also part of our everyday lives, from unlocking our smartphone to gaining access to our workplace and even being "tagged" in a photo on Facebook. Some recent uses of biometrics have triggered class actions relating to applying facial recognition technology to customer photos.

While we wait to see how the US courts will ultimately rule in these cases, the new EU General Data Protection Regulation (GDPR) brings biometric data for the first time into the special categories of data (classifying it as "sensitive"). This means that biometric data is now expressly regulated and subject to stricter processing conditions than other forms of personal data. In addition, the GDPR allows EU Member States to introduce further conditions on biometric data, which could mean further limitations under local law. Use of biometric technologies by commercial organisations in the EU has always been considered high risk from a data privacy perspective.

Top ten tips if you are considering biometrics

1. Establish if you are processing biometric data: Biometric data is data relating to an individual's physical, physiological or behavioural characteristics used "for the purpose of uniquely identifying a natural person" (Art. 9(1) GDPR). Examples include fingerprints, voice patterns, facial feature, retina or iris, gait pattern, palm feature, typing rhythm etc. Biometric technologies are therefore closely linked to identifiable individuals; the very purpose of these technologies is identification. Proceed with caution.

2. Have a clear purpose for processing: Proportionality and necessity are the key criteria applied by DPAs in assessing the fairness and lawfulness of processing biometric data. There must be a clear purpose for processing biometric data, and it must not be processed for any secondary purpose. DPAs are particularly sensitive about what is known as "function creep". This is where data is acquired for one purpose but used for another later. Ensure a clear and accurate definition of your "purpose".

3. Demonstrate no alternative methods possible: DPAs assess the lawfulness of an organisation's use of a particular biometric technology on the basis of any alternative methods that could be used which would have less of an impact on an individual's privacy. The biometric technology must be essential for satisfying the purpose (see Point 2 above) rather than being the most cost effective or operationally convenient. Organisations need to be able to demonstrate that a less privacy-invasive method is not available. This is a difficult test to satisfy.

4. Implement "Privacy by Design" measures: Processing of biometric data must be "adequate, relevant and not excessive", and the other usual data protection principles, such as accuracy, data minimisation and data security, must be upheld. It is preferable to store biometric data as a numeric "template" rather than in its actual "raw" form. A template is created as follows:

- A biometric sample, say a fingerprint, of the individual is captured.
- The unique features of this biometric sample are then extracted to create a biometric template made up of a binary code.
- The raw biometric data is then deleted from the biometric system and the template transferred onto either a smart card, local reader or a central database.
- The biometric system then matches the "live" fingerprint against the stored template in order, in the example of access control, to either authorise entry (if a positive match is made) or deny entry (if a negative match is made).

Regarding storage, DPAs are more likely to consider a smart card (or other similar device) that is exclusively held by the relevant individual as proportionate and lawful, and requiring less justification, than a central database or local reader. The optimal approach is storing a "template" on a card or something in the individual's possession.

5. Secure the data: Ensure that special safeguards and security measures (including encryption) are put in place to protect the link between the template and the raw, biometric data. It must not be possible for a third party to reverse engineer the template back to the original "raw" data. More generally, organisations must implement appropriate security measures to protect against unauthorised access to and disclosure of the biometric data (for example, by using cryptographic technologies). Access controls, such as a "need to basis" restriction, should also be put in place. If biometric data is stored on a database, make sure there is no linkage to other databases or systems.

6. Ensure accuracy: Biometric data must be accurate and kept up-to-date. Organisations should test biometric technologies / systems to ensure that false positives or matches are kept to a minimum. This also helps increase the security of the system (see Point 5 above).

7. Tell the data subject! The processing of biometric data must be

fair and transparent. Transparency is usually achieved by providing the individual (i.e. the data subject) with a notice which sets out the ways in which their biometric data will be collected and used by the organisation. The best time to provide this notice is before the biometric sample is taken.

8. Respect their rights! Individuals have certain rights in relation to their biometric data which must be respected by organisations at all times, including a right of access to such data, and a right to object to its processing.

9. Delete when no longer necessary: Biometric data should not be kept for longer than is necessary. In our access control example, when employees leaves the organisations, their biometric data should be deleted within a set period of time.

10. Carry out a PIA: Organisations should carry out a Privacy Impact Assessment (PIA) which will be a mandatory requirement under the GDPR. Also, keep an eye out for the Biometrics Institute's proposed Privacy Trust Mark which is currently in development phase.

AUTHORS

Nick Graham is a Partner and Jane Bentham an Associate at Dentons. Emails: Nick.graham@dentons.com Jane.bentham@dentons.com

Norway's DPA lacks independence says EFTA Surveillance Authority

The European Free Trade Association (EFTA) Surveillance Authority has issued a formal notice to Norway regarding the incorrect implementation of the EU DP Directive. The Authority says that Norway's Data Protection Authority is not fully independent in the sense that it cannot always make independent decisions about its work. The DPA and the Privacy Appeals Board are independent administrative bodies subordinate to the King and the Ministry.

"The Ministry issues a grant letter to the DPA each year, which highlights the priorities of the government in the field of data protection. According to the Norwegian Government, this grant letter serves as guidelines for the DPA's work, and sets certain priorities for the next year. In the grant letter for 2016, some of the aims for the DPA set out by the Ministry were, for example, to focus on Privacy by Design, and to ensure that data subjects and businesses that deal with personal data know or are familiarised with the applicable rules," the Surveillance Authority says.

In a similar cases against Germany, Austria and Hungary, the Court of Justice of the European Union (CJEU) held that the requirement of complete independence "must be interpreted as meaning that the supervisory authorities for the protection of personal data must enjoy an independence, which allows them to perform their duties free from external influence, direct or indirect, which is liable to have an effect on their decisions."

It therefore follows, in the case of Norway, that it has incorrectly implemented the DP Directive as regards the independence of the supervisory authority. The Norwegian government has been asked to submit its observations.

- *See www.eftasurv.int/media/esa-docs/physical/792769.pdf*

The EFTA Surveillance Authority monitors compliance with European Economic Area rules in Iceland, Liechtenstein and Norway, enabling them to participate in the European internal market. www.eftasurv.int/about-the-authority/the-authority-at-a-glance-/

Medical cloud service provider Quentry receives European Privacy Seal

Quentry, which enables medical professionals to share images, display the images in a web-based viewer and to add comments such as medical opinions in the cloud has received the European Privacy Seal as a recognition of its compliance with EU DP law.

The legitimate use of Quentry requires the collection of patients' informed consent and release from medical confidentiality and that they are obliged to verify the identity of other users in a reliable way prior to sharing medical information with them.

The evaluation focused on the examination of the multi-layered encryption solution that is employed. The result of the technical evaluation was that this solution approximates the level of a true end-to-end encryption to the greatest extent possible under the given circumstances. The solution used was developed by Brainlab, which manufactures and markets software-driven medical technology.

"Brainlab expended a great deal of effort in order to ensure the confidentiality of sensitive data" said Sebastian Meissner, Head of the EuroPriSe Certification Authority. "The comprehensive privacy hints that are provided to users of the service and Quentry's ability to de-identify metadata about patients are other positive aspects that deserve to be highlighted."

"Our goal was to go above and beyond the most stringent requirements for high-level data protection that customers and government regulators demand with Quentry" said Rainer Birkenbach, Executive Vice President at Brainlab AG. "We're pleased to see our efforts rewarded by EuroPriSe."

- *See www.european-privacy-seal.eu/EPS-en/Brainlab-Quentry*

Wearables and health apps need to win consumer trust and DPA acceptance

While search (Google) and social media (Facebook) have gained most attention in terms of tensions and legal conflicts with Data Protection Authorities, wearable technology and health apps companies are undoubtedly now feeling the pressure. **Stewart Dresner** and **Adèle Kendler** report from Barcelona and Brussels.

Much of the data wearable apps and health apps collect is sensitive data, and companies therefore need to be particularly careful about the legal basis for their data collection and the way that they gain the consent of their customers for the use of their data.

Technology companies are vulnerable to DPA attention[1] because they necessarily face two directions at the same time. They are driven by their commercial audience of investors and users who are looking for communications mentioning exciting product benefit words such as "connectivity… tracking your performance…heat map of users…sharing your data and social media presence". On the other hand, in Europe and in countries elsewhere with similar laws, companies need to engage with DPAs who are looking for understandable terms and conditions, a legal basis for processing, explicit consent for collection and use of health data for profiling as well as individual performance monitoring, transparency about sharing, risk of stalking, concerns about processing of data in a less rigorous legal environment, and data retention. Everyone is worried about external hacking, as a data security issue, but a contravention of data protection law covers a long list of issues in different jurisdictions. Companies new to the subject are often worried more about securing their intellectual property than providing rights to the individuals whose data they have captured.

Companies need a consistent privacy message

At the IoT Shifts Conference[2] in Barcelona in October last year, Mathew Davis, Product Director, Experience Innovation, from Nike headquarters in Oregon, spoke to an audience of Internet of Things enthusiasts and innovators. The company has developed smart running shoes which monitor the wearers' performance compared with others, and their location appears on a heat map of popular running routes in many different areas. He said that these technologies are useful for both elite athletes and millions of ordinary runners. The technologies assist with providing data for product enhancements, and understanding the impact of different temperatures on runners' performance. When *PL&B* asked whether Nike could track an individual, the answer was no.

However, at the CPDP Conference[3] in Brussels in January this year, it became clear from a presentation by Sjoera Nas, Senior Inspector for the Netherlands DPA, that Nike, unsurprisingly, does indeed collect individual data points in order to construct its individual performance data, groups' shared data and aggregate data sets.

Why did the Netherlands DPA take the lead?

Nike's European headquarters is in the Dutch town of Hilversum, and its Running App has been downloaded millions of times to both Android and Apple devices in the Netherlands and elsewhere in Europe. Therefore, it is not surprising that Nike's privacy policy for its Running App was subject to investigation by the Netherlands Data Protection Authority last year (*PL&B International,* December 2015 p.23).

The Netherlands DPA found that users of the App had not been given sufficient information on how their health data was being processed and that explicit consent had not been obtained. In addition Nike did not inform users that their personal data was being processed for analytical and research purposes.

Users of this App are able to keep track of their running activities by, for example, measuring distances run, their speed and number of calories burned. Personal performance can be improved via the App by using personal training programmes, for which the App uses the GPS and network-based location data from the phone, and the acceleration sensor (accelerometer). The App allows users to share their runs and photos with friends and enter competitions.

Nike's new European privacy policy

As a result of discussions, in which the company's lawyers discussed the issues in detail, the company published a new Privacy Policy and Cookie Policy (Europe)[4] in January this year in which they plugged the gaps. Although the Netherlands DPA lacks fining powers, this result achieved most of what the DPA was seeking; a privacy policy which met the requirements of both the EU Data Protection Directive and Dutch law.

As the issues with Nike as a global brand are the same across Europe and indeed the world, *PL&B* put some questions to both the Netherlands DPA and the company – see boxes.

Other health apps and regulatory advice

Companies experienced with privacy issues, such as Microsoft, are more likely to develop privacy policies for its fitness wrist bands[6] without attracting

THE NETHERLANDS DPA'S PERSPECTIVE

Merel Eilander, Senior Spokesperson, provided the answers for the Netherlands Data Protection Authority

***PL&B*: Did you conduct this investigation as a result of complaints or on your own initiative?**
DPA: At our own initiative. We generally keep an eye on apps that are popular in the Netherlands, with a focus on health and fitness apps.

***PL&B*: Was this investigation solely a Netherlands DP Authority initiative or was it part of a wider European exercise, as with France's CNIL's investigation of Google, and Ireland's DP Commissioner's and Belgium's Privacy Commission's investigation of Facebook?**
DPA: No, this investigation was conducted solely by the Netherlands DPA because Nike has its European headquarters in Hilversum, in the Netherlands.

***PL&B*: Have you conducted any follow-up work to check the extent to which Nike in the Netherlands is changing its data collection and privacy policies and practices as a result of your investigation and report? If so, how?**
DPA: Yes, we are currently supervising the implementation of measures described by Nike to end the ascertained violations of the Netherlands data protection law. Some measures are already publicly visible, such as the introduction of a new privacy policy from 1 January 2016, and an e-mail alert to existing users. We cannot disclose any further details at this point in time.

***PL&B*: Have you cooperated with other national DP Authorities to ask whether Nike has amended its privacy policy and data collection methods in other countries? If so, in which countries?**
DPA: No, we have not specifically asked other DPA's about possible national differences in the personal data processing with the Nike+ Running app. Generally, Nike has one privacy and cookie policy for Europe, and it does not seem likely to us, based on Nike's cooperation with the investigation, that they would apply different rules in different countries in the EU.
We have of course informed our colleagues in the EU Article 29 DP Working Party about the results of our investigation. By publishing the results of our investigation in English,[5] we generally welcome feedback from any colleague DPA or other interested party.

A NIKE SPOKESPERSON'S PERSPECTIVE

***PL&B*: Has Nike in the Netherlands changed its data collection and privacy policies and practices as a result of the Dutch Data Protection Authority's investigation and report? If so, in which ways?**
Nike: Nike takes the protection of consumer data very seriously. We welcomed the opportunity the Dutch Data Protection Authority (DPA) provided to enhance the experience for our users while also taking additional steps to protect the information they share with us.

***PL&B*: Has Nike amended its privacy policy and data collection methods in other countries? If so, in which countries?**
Nike: The Nike+ Running application was designed to provide consumers with the analytical tools to help them reach their athletic potential. Nike uses height and weight data inputted by athletes into the Nike+ running app for accurate calorie and distance calculation. Nike uses fitness data to track runs and to provide aggregate comparisons to users of similar age and gender within the app.

***PL&B*: Has Nike communicated the Netherlands Data Protection Authority's findings internally or responded externally? If so, how, to whom, and in which countries?**
Nike: We develop our applications to comply with the laws of countries in which we operate and believed our Nike+ Running app was in full compliance with Dutch law. Based on the Dutch DPA's explanation of what qualifies as personal health data, we are working closely with them to understand the recommended updates. This process is ongoing but has already included the redrafting of our European privacy policies to incorporate their recommendations.

attention from DPAs. But less experienced developers of health apps now have much more guidance than in the past.

The European Data Protection Supervisor on 21 May 2015 published an 18-page Opinion titled "Mobile Health: Reconciling technological innovation with data protection"[7]. The summary includes the following advice for app developers: "app designers and publishers should design devices and apps to increase transparency and the level of information provided to individuals in relation to processing of their data and avoid collecting more data than is needed to perform the expected function. They should do so by embedding privacy and data protection settings in the design and by making them applicable by default, in case individuals are not invited to set their data protection options manually, for instance when installing apps on their smart devices."

The European Commission, as part of its work on Digital Economy and Society, published at the end of May 2016 the second iteration of a draft health code for app developers, Current initiatives to unlock the potential of mobile health in Europe[8]. It includes sections on data protection and consumer law and is open for comment. The 71-page document states in its introduction "The purpose of the mHealth app assessment guidelines is to establish a framework of safety, quality, reliability and effectiveness criteria to improve the use, development, recommendation and evaluation of mHealth apps." The list of organisations involved in this initiative was updated on 2 June.

The EU Art. 29 DP Working Party Work programme 2016 – 2018 (adopted 2 February 2016) (417/16/EN WP235), included a statement that the Technology subgroup "will continue its work together with other subgroup(s) when appropriate on the following topics:…."user friendly and privacy-compliant ways of informing and expressing consent by way of smart devices".[9]

Meanwhile, companies of all sizes are embracing opportunities presented by innovative products and services. Examples given at the CPDP Conference session on wearables were from the pharma and insurance sectors.[10]

Cecilia Alvarez Rigaudias, European Data Protection Officer at *Pfizer* spoke at the CPDP Conference about how the company is sponsoring trials of apps which help doctors monitor patients' behaviour regarding consumption of food, pills and engaging in exercise routines which can assist in a

diagnosis and remind patients of their medical appointments. The company needs to be careful because apps are not developed with privacy in mind, native security settings are poor, and users are not well educated into how to use the apps. If app developers do not collect data correctly, Pfizer does not want to have such data on its servers.

Gwendal Le Grand, Director, Technology and Innovation at the *CNIL*, France's DPA, reported that AXA, an insurance company, and Withings, an IoT device company, have a partnership in France. People are supplied with a Withings Pulse pedometer with which they can prove that they are achieving their typical target of 7,000 or 10,000 steps per day for a month. If so, they will earn a discount coupon for the renewal of their health insurance policy and discounts for other Withings products.[11]

The future

Innovations in wearables keep appearing beyond smart watches and wrist bands from well-established companies. A Montreal, Canada-based company, OMSignal, sells men's washable smart running shirts which pass performance data to the cloud, like a fit band. The same company, on 3 January this year, announced the release in the first half of 2016 of the OMBra – a smart bra for women who want comfort and the same performance data as men.[12] The company has a privacy policy presumably drafted for North America[13] but it will need further work to make it reach the stricter requirements of the EU Data Protection Regulation. It is the type of IoT health app and service which was the subject of the survey by the CNIL and the Privacy Commissioner of Canada in April this year.[14]

"Connected devices, such as fitness trackers, smart scales, sleep monitors and other health related products, are capable of capturing some of our most intimate data," said *Commissioner Daniel Therrien*. "Given the sensitivity of the information, it is imperative that the companies behind such devices are transparent about what they collect, how the information will be used and with whom the data will be shared. I'm pleased the Sweep will focus on this important area under the Internet of Things banner."

In the wings are a host of start-ups supported by investors. One such wearable company is Enflex[15]whose website makes impressive claims for the product "Enflux smart clothing has 10 embedded 3D motion sensors. Simply put on Enflux and record the full motion of your body while you exercise. Our app provides real-time, actionable feedback on how to improve your athletic performance, just like a coach." However, in addition to there being no privacy policy information on the website, there seems to be no information about the company itself.

AUTHORS

Adèle Kendler is a *PL&B* Correspondent. Stewart Dresner is *PL&B's* Publisher.

REFERENCES

1 The Global Privacy Enforcement Network (the group of 59 Data Protection Authorities across 43 jurisdictions) conducted a sweep (survey) in April of privacy aspects of the Internet of Things (IoT) products and services. www.privacyenforcement.net/about_the_network
2 www.claropartners.com/iot-shifts-conference-2015/
3 www.cpdpconferences.org/
4 Nike Privacy Policy and Cookie Policy (Europe) - updated January 2016 http://help-en-eu.nike.com/app/answers/detail/a_id/56560/p/5593
5 See www.cbpweb.nl/en/news/translation-press-release-10-november-2015-nike-modifiesrunning-app-after-dutch-dpa and conclusions of the investigationat https://cbpweb.nl/sites/default/files/atoms/files/conclusions_dpa_investigation_nike_running_app.pdf
6 https://privacy.microsoft.com/en-gb/privacystatement updated January 2016.
7 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf
8 https://ec.europa.eu/digital-single-market/en/news/current-initiatives-unlock-potential-mobile-health-europe
9 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm
10 A YouTube video of the CPDP Conference wearables session is at www.youtube.com/watch?v=8G8jaouXbLk
11 www.rudebaguette.com/2014/06/02/reduce-health-insurance-bill-tracking-steps-wearables/ and www.axa.fr/mutuelle-sante/partenariat-withings/jeu-pulse.html
12 www.omsignal.com/blogs/omsignal-blog/81228673-introducing-the-ombra-and-the-all-new-omrun-platform
13 www.omsignal.com/pages/privacy-policy
14 www.priv.gc.ca/media/nr-c/2016/nr-c_160411_e.asp
15 www.getenflux.com/

Cayman Islands is preparing data protection bill

The Cayman Islands in planning to adopt an EU-style data protection law in the autumn, the Cayman Compass reports. It is expected that an amendment bill will be brought before parliament in September.

"The legislation is part of a package of legal changes the Progressives-led administration is contemplating in order to fall in line with European directives related to privacy protection and tax information exchange," the Cayman government said.

Cayman Premier, Alden McLaughlin, said the EU Data Protection Regulation had raised some concerns with the local financial services industry.

"Acknowledging privacy as a basic human right, in September new data protection legislation will … be introduced that is on par with what is in place in the European Union," the government statement said.

• *For more details see www.caymancompass.com/2016/05/11/data-protection-legislation-put-off-until-fall/*

The EU DP Regulation countdown has started

Two years from now, organisations will have to be ready to comply. The UK will be challenged by the EU DP Regulation whatever happens in terms of EU membership following the UK's in-out referendum on 23 June. By **Laura Linkomies**.

PL&B's seminar on the newly adopted EU General Data Protection Regulation (GDPR), organised jointly with law firm Browne Jacobson in London on 25 May, revealed that there are still many grey areas. Neither businesses nor lawyers are completely sure what the legislator wants, or what the rules will be in areas that allow for national manoeuvre.

Stewart Dresner, *PL&B's* Chief Executive, said: "The EU DP Regulation entered into force 24 May – so in EU language this means that Member States cannot do anything contrary to the legislation, but organisations now have two years to prepare. The law is enforceable from 25 May 2018. There is some room for national discretion in the form of exemptions – many aspects were controversial during the negotiations and this is the result."

"In terms of national interpretation in the UK, I do not expect any radical changes when the new UK Information Commissioner, Elizabeth Denham, starts her term this summer. In terms of possible Brexit, I also do not expect many changes for data protection – even if the UK were outside the EU, business needs to have a data protection law consistent with the rest of Europe."

Mark Gleeson, Partner at Browne Jacobson said that he agreed. The EU already has the view that the UK has not transposed the EU DP Directive correctly. Should Brexit happen, the UK would be deemed as non-adequate, and would have to apply for an adequacy decision and effectively implement the Regulation to be in that position.

What to do now?

Richard Nicholas, Partner at Browne Jacobson talked about what organisations need to do differently in the UK once the EU DP Regulation takes effect. "It will completely supersede the previous UK DP Act and the EU DP Directive. As we now have a Regulation, it will have direct effect on Member States. This is generally a good thing as it allows for harmonisation, but there is some scope for national implementation in some areas, for example with regard to children's data. For the first time, data processers are affected – this will have a huge impact on the technology sector. The IT industry has not quite opened up to this fact yet. It does not matter where the data is processed, but whose data it is. EU citizens' data is protected even if the controller or processor is outside the European Economic Area (EEA) if supplying goods and services, or monitoring their behaviour. This will have an impact for instance on cloud computing providers who are often outside the EEA."

So what is new? The accountability principle, breach notification and greater transparency obligations are all new aspects. It will be harder to achieve data subjects' consent and generally there will be a wider inclusion of personal data within the scope of data protection law, Nicholas said. Personal data will include cookies, and ways by which an individual can be identified.

Data protection will become an important area for insurance due to mandatory data breach notification. Also reporting requirements and sanctions for breaches are considerably more significant than before, Nicholas said.

Lauren Millward, Solicitor at Browne Jacobson, said that new individual rights and the new accountability principle mean that data controllers need to revise their compliance programmes carefully: "Under the current law, Subject Access Requests (SARs) have to be responded to within 40 days, whereas the new requirement is one calendar month. More information will have to be provided in the privacy notice. Practical considerations include where to provide the privacy notice. If collecting data indirectly, say by a third party, organisations are still required to provide this information – so check any third party contracts. Storage of data is also an issue – do you have a retention policy? When responding to a SAR, you need to supply information about the envisaged retention period."

If an individual requests their data to be deleted, this right needs to be balanced with Freedom of Information considerations, Millward said.

"Data portability applies only when processing is based on consent and is automated. Data is provided to another data controller, for example, when an individual wants to change bank accounts. Practical considerations include the difficulties with separating out relevant data. As data has to be provided in a machine readable manner, it is worth checking now your IT capabilities."

An area of concern for industry is to provide information transparently. How to inform people of processing when they are using an app? Icons were suggested by the EU at the time of the first draft of the GDPR but nothing has been agreed. Organisations may create their own icons if they are helpful in communicating information to individuals.

There was a lengthy discussion on profiling. If linked with marketing, can organisations tailor communications based on preferences? What is the legal effect? Gleeson said that there is a lack of clarity here. Profiling is clearly important for marketers. It is very powerful but can be legally acceptable if organisations are doing the right thing for the consumer.

Changes ahead for UK business

Ian Bourne, DP Policy Delivery Group Manager, the ICO, said: "The

ICO's traditional ability to be flexible and business savvy will be under much more scrutiny from other DPAs and the European Data Protection Board (EDPB) as well as the European Commission. So we will have some challenging times internationally – our approach and guidance may be challenged."

"The Regulation has some mistakes in it and even typos, and things that do not work so well. But it is much better than it could have been." The UK government was very effective in lobbying and getting some of the aspects omitted that would have been undesirable, Bourne explained.

"We now have a reasonable picture of which aspects business has issues with, and this will be reflected in our guidance. We have to make changes within the ICO to prepare for breach notification and prior authorisation for the processing of sensitive data, which are new duties for us. Also Elizabeth Denham, the new Commissioner, is starting mid-July."

"The Regulation has direct effect. But we also have around 40 areas where EU Member States can exercise national discretion, for example, national security, crime prevention, freedom of expression, such as whether citizen bloggers can enjoy the journalistic exemption. I imagine that the government wants to keep these issues as similar to the current position as possible."

Bourne said that the Department of Culture, Media and Sports (DCMS) is now working on the UK law – how to marry the Regulation text with national interpretation of the exemptions.

Also the Article 29 Group is now very busy – it is trying to issue guidance on many topics that they have prioritised – for example Data Protection Officers (Dutch and French DPAs are rapporteurs for this topic). The ICO is working on a paper on the consistency mechanism.

"We are trying to get the Art. 29 DP Working Party to reform itself – the European Data Protection Board (EDPB) will be very different, as it can issue binding decisions, and the UK can be outvoted by a majority of the members. We try to encourage the group to conduct more consultations with stakeholders. There has been some success."

Bourne cited as an example Google Streetview which caused some controversy amongst DPAs, and was deemed illegal in France. In some countries Streetview was launched, but some German Lander (states) banned it. If that happened under the GDPR there would be a vote and a differing UK view would be outvoted. "We will have to bring these messages to business which will be difficult," Bourne said.

"The ICO will issue guidance soon, first on the main practical aspects to point out differences between the current law and GDPR. An automated breach notification system is being developed. We are a little concerned that prior notification for risky processing and breach notification may cause over-notification of trivial incidents so the IT system should weed some of that out."

He explained that there would be a matrix to gather details on the breaches – number of records lost, their sensitivity etc. Non-security breaches would also be covered – a breach does not always include loss of data.

Bourne said that the ICO will carry on investigating complaints. Some other DPAs, such as the Netherlands, do not conduct any outreach educational work and some countries' DP Authorities handle few or no complaints whereas the ICO handles 30,000 – 40,000 complaints a year. Bourne said that GDPR will make a huge difference to fines. The biggest fine the ICO has ever issued was £450 000. However, some other DPAs, particularly Spain, have traditionally issued large fines. Under the EDPB, any fine that the ICO issues can be challenged if the other DPAs think it is too low. The Article 29 Data Protection Working Party is now working hard to get the Board running and agree on the rules – how to conduct voting, for example.

Bourne said that the ICO is still working on its own privacy seal, which has proven to be quite a challenge, for example, with trademark issues. Doing the same at EU level would be difficult and time-consuming, he said.

Another issue where EU DPAs have differing views is profiling. There are very different types of profiling. We think that some profiling is very benign, Bourne said. Other DPAs take a different view. "Trying to get people understand there are different types of profiling will be difficult to do. It is important for companies to be sensitive as to what is 'creepy'."

Public sector issues

Megan Larrinaga, Solicitor at Browne Jacobson, spoke about implications for the public sector.

She suggested that they should, in the first instance, do three things;

1. Analyse the basis on which personal data is processed. Legitimate interest exemption will no longer be available. Is processing necessary in the public interest however?
2. Consider the rights of the data subject; how to deal with unrealistic expectations? Data controllers are entitled to reject vexatious requests.
3. Prepare for data breaches. Who would be on a response team? Training exercises are useful.

International aspects

Stewart Dresner spoke about international transfers under the GDPR, reiterating the adequacy requirement and the countries that have so far been declared "adequate" by the European Commission. In December 2015, South Korea applied and Japan in considering applying. Standard contractual clauses are rigid but legally sound as a legal basis for transferring personal data from the European Economic Area to third countries, Dresner explained, and therefore companies have been looking into Binding Corporate Rules but they are time-consuming and expensive in resources. Until we have the EU-US Privacy Shield in place, companies should continue to use these tools. "But it is best to review your use of personal data, and assume that even if adopted, the Privacy Shield is likely to be challenged in the Court of Justice of the European Union," Dresner said.

Richard Nicholas spoke about cloud and outsourcing. He said that some aspects are changing under the

GDPR. While data controllers are still ultimately responsible for compliance with the GDPR, data processors and even sub-processors are also responsible. But who takes responsibility for what? The One-Stop-Shop across the EU should ensure a consistent approach.

Organisations will need more detailed written agreements. Both processors and controllers need to keep records. The controller has to ensure Privacy by Design, but the processor also has similar obligations. He said that organisations should now review cross border data flows, keep records of third party processing, and review agreements.

New consent requirement

Valerie Taylor, Principal Consultant at *PL&B*, explained how the consent requirement under the GDPR differs from the current situation. Consent must be freely given and unambiguous. This means some sort of positive action by the data subject. Consent can be withdrawn any time – but this does not affect processing that has already happened. If your provision of services is dependent on consent, it can be a weak legal basis for the processing of personal data. You will need an audit trail to show how and when consent was obtained.

In the future, businesses need to inform individuals about the legal bases of processing, including the legitimate interest of the controller, Taylor explained. Also they need to provide information on which data processors they use – but clearly cannot include all of them. It is not yet clear how to interpret this provision.

"The only way this can work is to continue to use layered privacy policies" Taylor said. "But what is essential information?"

Mark Gleeson talked about data breach notification, a new responsibility under Art 33 in the GDPR. Notification to the ICO will be required without undue delay and where possible, within 72 hours. Notification is not required if unlikely to result in risk to rights and freedoms of individuals. Processors have to notify controllers. In some cases, notification is also required to the individuals concerned.

INFORMATION

This seminar will be run again in Birmingham on 28 September 2016. For more information and to register go to www.privacylaws.com/Events/Other/EU-Data-Protection-Regulation-Time-to-get-organised-in-the-UK1/

The ICO's GDPR microsite, which has its 12-point plan, is at www.Dpreform.org.uk

United Nations issues study on data protection and trade

The United Nations Conference on Trade and Development (UNCTAD) published on 19 April a major new study, *Data protection regulations and international data flows: Implications for trade and development*.

The United Nations is emerging as an important voice in the data protection debate, with the ability to engage with developing nations and emerging markets. In the last three years they have taken an active interest in data protection: in 2013 they issued the Statement on the Right to Privacy in the Digital Age; in 2014 they published a detailed report on human rights and privacy online; and in 2015 they appointed a Special Rapporteur on the Right to Privacy (see p.28).

This new report, released as part of the UN E-Commerce Week in Geneva, is a major study (170 pages) examining the relationship between data protection and trade, with a strong focus on the issues faced by developing nations. Chris Connolly, Director, from Galexia, was the lead author / consultant for the study, but the study also includes detailed contributions from national governments, regulators and businesses - including notable contributions from developing countries (Benin, Ghana, Mauritius, Niger and Uganda).

The study identified numerous challenges in the development and implementation of data protection laws, including:

1. Addressing gaps in coverage
2. Addressing new technologies
3. Managing cross-border data transfers
4. Balancing surveillance and data protection
5. Strengthening enforcement
6. Determining jurisdiction
7. Managing the compliance burden.

The study includes practical policy options and suggestions for global, regional and national stakeholders. The UN tries to promote a balanced, pragmatic approach on these issues, stressing the importance of maintaining international data flows and avoiding fragmentation.

The report encourages countries to adopt comprehensive baseline privacy protection, based on common principles, with strong enforcement. However the report also encourages countries to include options for the cross border transfer of data, and to tackle the issue of balancing privacy against surveillance 'head on', by establishing rules for necessary and proportionate surveillance, complemented by judicial redress and oversight. The report provides an interesting perspective on the global data protection debate, which is so often dominated by issues in the US and EU.

Reported for PL&B by Chris Connolly, Galexia www.galexia.com

• *Professor Graham Greenleaf, PL&B Asia Pacific Editor, and Professor Ian Walden, Queen Mary, University of London, are contributors to the report. The full report, published on 19 April is available at http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf*

Central and East European DPAs challenged by new technologies

Jiří Maštalka reports from the 18th meeting of the Central and Eastern European Data Protection Authorities in Sarajevo.

Bosnia's Personal Data Protection Agency hosted, in Sarajevo, the 18th meeting of the Central and Eastern European Data Protection Authorities (CEEDPA) on 11-12 May. The other participants were representatives from Data Protection Authorities of the Czech Republic, Bulgaria, Hungary, Georgia, Slovenia, Macedonia, Serbia, Poland, Croatia, Slovak Republic, Albania, Moldova, Russian Federation, Bosnia and Herzegovina, Montenegro, Kosovo[1] and the Council of Europe. Armenia was accepted as a member of CEEDPA in the course of the meeting.

The meeting focused on practical issues related to some topical activities of the Data Protection Authorities.

Video surveillance in public and private sectors

The participants confirmed that while the data protection acts are technologically neutral, some countries have adopted specific regulations related to video surveillance, especially for the purpose of personal security and protection of property. Thus, the provisions of general data protection acts are fully applicable to processing of personal data via video surveillance.

Special cases of video surveillance are, as mentioned by the delegate of the Czech Republic, cameras installed on unmanned aircrafts (drones). An easily available combination of cameras and aircraft constitutes outstanding technological progress. On other hand, this technology represents a new, very flagrant threat to the privacy of citizens. It is possible to systematically capture and further process shots of identified or identifiable natural persons, including in a purely private environment in which these persons are present or live (gardens, flats, and so on). Consequently, it is possible to acquire personal data in a relatively easy manner from an environment that would otherwise be very difficult to access.

This is a new conceptual issue and it is posing a problem in itself. Access to an area must be, from a legal point of view, viewed two-dimensionally, in terms of horizontal access. Thus, the surface of a public square accessible to anyone in the above manner shall be a public space, but is not a private garden that is visually accessible from the air, regardless of the fact that an unmanned aircraft discloses the third – vertical – dimension.

The operator of an unmanned aircraft, (in the case that shots of identified or identifiable persons are made with the purpose of using them to identify specific persons), will be in the position of a controller or processor and must therefore respect the following basic rules. Above all, such an entity must not make recordings of purely personal activities (in particular within a residence and adjacent areas) or recordings that would primarily serve to humiliate human dignity.

> How to find the right balance between the legitimate interests of an employer and the rights of an employee?

Furthermore, recording must be based on at least one of the legal grounds under the Personal Data Act:

- consent of the data subject (although it is a relatively rare case where consent is applicable to some community like spectators at a stadium);
- executing tasks required by law (for instance the police);
- protection of the rights of the controller or other persons;
- protection of the vitally important interests of the data subject.

Immediately following the recording, controllers need to determine whether all shots containing personal data serve the stipulated purpose and ensure that excess recordings (or parts thereof) are destroyed. The Czech Data Protection Authority has dealt with the first set of these cases and expects to receive others in the future.

However, the identification of the controller, namely the operator of the aircraft or the provider of a video surveillance system, is the weak data protection link in this field.

Data processing in the field of employment

A crucial task in this field is, according to the opinion of the delegate from Serbia, finding the right balance between the legitimate interests of the employer and the personal rights of an individual employee when determining whether personal data processing is legal or not. As a consequence of the overwhelming imbalance of power between the employer and the employee, in order to get or to keep a job, the employee is willing to put his privacy and his personal data at the disposal of the employer. An imbalance of power between the parties, and the toxic environment that is present in the labour market, raises questions about the legality of the consent. Thus, a key problem is excessive data processing and processing without a clear purpose.

A very interesting case related to monitoring a specific employee was mentioned by delegates from Slovakia. The data controller used localization services through a person acting in their name (an entitled person). The service may be activated whenever it covers territory of the Slovak Republic with a GSM signal of a telecommunication

operator. It collected the approximate location of the smartphone (street and city) and the exact time. The controller used the collected data to file a lawsuit against this employee in order to support their statements that the employee did not fulfil their duties and seriously infringed working discipline. Before initiating the service, the controller unsuccessfully tried to contact the employee in order to check his physical presence in the workplace. The Slovak Data Protection Authority concluded that the controller processed data pursuant to Section 11 of the Labour Code. However, determining the conditions of the processing of geographical location data without taking into account working hours and time off may harm a data subject's rights. Thus, the DPA imposed an obligation to determine the conditions of the processing, for example, by amending internal policies that adjust rules and conditions for employee monitoring, and ensuring that only such geographical location data are processed, the extent and contents of which correspond with the stated purpose.

The Council of Europe delegate introduced "The Council of Europe Recommendation 2015(5) on the processing of personal data in the context of employment" and the Bulgarian delegate presented the publication "Privacy protection in the workplace - Guide for employees", developed as a result of the Leonardo da Vinci Partnership Project in cooperation with experts representing Data Protection Authorities of Poland, the Czech Republic, Croatia and Bulgaria.

Collection and processing of biometric data

The Slovenian delegate stressed the need for strict rules for the processing of biometrics data, especially in the private sector. In Slovenia, the private sector may implement biometric measures only if they are required for the performance of activities, for the security of people or property, or to protect secret data or business confidentiality. Biometric measures may only be used on employees if they were informed in writing in advance.

The Hungarian delegate referred to facial recognition as an example of biometric data collection. The delegate explained that the processing of photographs will not always represent processing of special categories of personal data as they will only be covered by the definition of biometric data when being processed through a specific technical means that allows the unique identification or authentication of an individual.

The delegates said that there was an increasing number of processing operations over biometric data for the purpose of employee monitoring, for instance, the processing of fingerprints for the purpose of evidencing the presence of an employee at the workplace. The Serbian delegate mentioned a complaint from a union of a state utility company. A director installed a program on all the employees' computers which tracks their activity. The Commissioner conducted an investigation and found out that the program traced keystrokes, made screenshots and logged activity. The system was being implemented in order to prevent misuse of resources and to tighten discipline. Employees were verbally informed that "everything will be tracked". The Commissioner concluded the data processing was excessive for the defined purpose.

Russian approach to data subjects' rights

According to the opinion of the delegate from the Federal Service for Supervision of Communications Information Technology and Mass Media (Roskomnadzor) the Russian model harmoniously combines elements of the European and Asian approaches (The Asian approach was originally reserved for the state with its administrative and repressive mechanisms for the protection of citizens' rights). In less than 10 years from the establisment of the data protection institution, it has developed its own methods of regulating personal data processing. The Russian Authorized Body for the Protection of Data Subjects has a number of powers, including conducting control activities, considering citizens' appeals, appealing to courts for protection of data subjects' rights, as well as prosecuting persons guilty of violation of the personal data legislation. As a response to challenges and threats of the digital environment, Russia adopted, in 2015, the Data Localization Law. Such a mechanism to solve the problem is unique, since it establishes the duty to localize all personal data. This national localization is designed in such a way that it does not contradict the nature of the Internet, nor does it cancel or prohibit cross-border transfer of data, the Russian representative said. The main objective is not to punish the operator financially, but rather to promote the building of a system of personal data processing in a company that will meet the requirements of the Law. Roskomnadzor launched in 2015 a number of awareness-raising projects.

The participants said the meeting was a unique opportunity for the exchange of experiences and expressed thanks to Bosnia's Personal Data Protection Agency for its excellent organization. The host of the next CEEDPA meeting will be Georgia.

AUTHOR

Jiří Maštalka is a lawyer in the Legal Department at the Office for Personal Data Protection (OPDP), The Czech Republic.
Email: jiri.mastalka@uoou.cz

INFORMATION

The OPDP's Annual Report in English, with case studies and statistics, was published on 18 May. The current President, Ms Ivana Janů, was appointed as the new President of the Office for a period of five years starting on 1 September 2015.
www.uoou.cz/en/

REFERENCES

1 Without prejudice to position of status, in line with UNSCR 1244 and the ICJ Opinion on the Kosovo declaration of the independence.

Philippines appoints Privacy Commission in time for massive electoral data hack

The Commission will soon issue implementing rules and regulations.

By **Graham Greenleaf**.

The Philippines Data Privacy Act 2012 (DP Act) was signed into law by President Benigno Aquino on 15 August 2012, and (in theory) came into effect 15 days after its publication (s. 45). The Act remained dormant, because until a National Privacy Commission (NPC) was appointed, and made Implementing Rules and Regulations (IRR), very few of its provisions were enforceable, and none were enforced. After nearly four years, the NPC has finally been appointed, and has taken up its role at a time of change of Presidents, combined with a massive data breach at the country's electoral commission (Comelec). This article surveys this changed landscape, and the implications for businesses of the delayed coming into force of the Philippines' law.

Philippines law awakes: Commission appointed

On 8 March 2016, less than four months before the expiry of his Presidential term, Aquino finally appointed the three-person Commission, each for a three year term (with possibility of re-appointment for a second term).[1] Raymond Liboro, a public servant previously working as Assistant Secretary of the Department of Science and Technology (DOST) and officer-in-charge of the DOST's Science and Technology Information Institute, is the Privacy Commissioner, leading the three-member Commission. The two Deputy Privacy Commissioners are Ivy Patdu, an attorney and medical doctor specializing in health information exchange, and Dondi Mapa, a technology professional. All three members of the NPC are appointed by the President for a term of three years. They may be reappointed for another term of the same duration.

The law specifically put the Commission under the Department of Information and Communications Technology (DICT), with the caveat that if it comes into law before a DICT was established, the Commission will come under the Office of the President. No DICT has been established. However, Philippines sources speculate that since it was Department of Science and Technology (DOST)'s secretary Mario G. Montejo who administered Liboro's oath, it appears that the NPC is now under the DOST.[2]

NPC's first test: Comelec mega-hack

Less than a month after the NPC's appointment, on March 27, the Commission on Elections (Comelec) website was hacked and defaced, allegedly by the group Anonymous Philippines, and its database containing personal identifiable information of 55 million voters was copied. All of the contents were posted online by another group, LulzSec Pilipinas, available for public downloading.[3] The data apparently comprises 228,605 email addresses, 1.3 million passport numbers and expiry dates of overseas Filipino voters, and 15.8 million fingerprint records, plus physical address, place of birth, height, weight, gender, marital status and parents' names (all non-encrypted), and other data, such as first and last names and dates of birth, which were encrypted.[4] A 23-year-old IT graduate has since been arrested and charged under provisions of the Cybercrime Prevention Act concerning "illegal access to the whole or any part of a computer system without right."[5] The Data Privacy Act also includes penalties for such hacking actions, an unusual feature of a data privacy law in that they are aimed at third parties, not data controllers.

> Unlike the data protection laws of Singapore and Malaysia, the Philippines Act covers the public sector.

Unlike the data protection laws and commissions in the ASEAN neighbours of Singapore and Malaysia, the Philippines Act covers the public sector, and the NPC can investigate the public sector. Under the Data Privacy Act, a public sector data controller such as Comelec must promptly notify the NPC when personal information is believed to have been acquired by an unauthorised person and a real risk of serious harm is likely to result – circumstances satisfied here. Even though the Act is not yet fully in force, the National Privacy Commission has started an investigation and received an initial report from Comelec. The first test of the NPC will be its investigation of the adequacy of the security procedures of Comelec.

Implementing Rules and Regulations (IRR) required

The NPC must make implementing rules and regulations (IRRs) within 90 days of its appointment, but then "[e]xisting industries, businesses and offices affected by the implementation of this Act" are given one year from the effective date of the IRRs (or such

other period as the NPC may determine) to comply with the requirements of the Act' (s. 42). So the IRRs must be made by early June 2016, and it will be June 2017 before businesses and agencies must comply (except in the unlikely event of the NPC setting an earlier date).

The DP Act does not specify what matters the IRRs must cover. A law firm has suggested that they will cover such uncertain matters as "the scope and extraterritorial application of the law; duties and obligations of personal information controllers and personal information processors, especially companies engaged in business process outsourcing in the Philippines; mechanism for concerned companies to appoint a data privacy officer; and procedure for concerned parties to notify the NPC if sensitive personal information in their custody were acquired by an unauthorized person, and other reportorial requirements".[6]

Powers and functions of the NPC

The NPC is stated to be "independent" (s. 7). There are no provisions allowing ministers to give it directions, although nothing is specified concerning removal of Commissioners from office, or provision of a budget. The extent of its actual independence will need to be assessed in practice, and in light of its resources.

The NPC has a considerable range of enforcement mechanisms, but they are generally marred by confusing drafting, apparent gaps, and lack of procedural detail. Failure to comply with any of the principles in the Act could result in a complaint investigation by the NPC (once the IRRs are in force), but only a specific sub-set of breaches can result in prosecutions under Chapter VII "Penalties". The NPC has a general function of "ensuring compliance" by controllers with the Act (processors are not mentioned) (s. 7(a)), with ample powers to investigate and mediate. The NPC cannot issue administrative penalties or fines, and can recommend prosecution by the Department of Justice for only some breaches of the Act. Illogically, there are some other offences where the NPC cannot even recommend prosecution.[7] The NPC has no powers to award compensation. Actions for damages ("restitution") may also be possible via the courts in an action under the New Civil Code, but the Act only provides for this when an offence has been proven (s. 37).

The NPC also has a wide range of other functions (s. 7). It can give advisory opinions on the meaning of legislation, can comment on proposed legislation, and can propose legislation (s. 7(i)-(m)). It is supposed to provide a compilation of government agency record systems (s. 7(h)), but is unlikely to do so unless it is given considerable resources. The NPC can also approve (or reject) voluntary privacy codes, which can include private dispute resolution mechanisms (s. 7(j)). The consequences of such approval on the operation of the Act are not specified, so this provision seems incomplete and ill-considered (the IRRs may be able to remedy this). It can coordinate with overseas privacy regulators and 'private accountability agents' and participate in international and regional privacy initiatives (s. 7(n)-(q)). The Asia-Pacific Privacy Agencies (APPA) meeting in Singapore in July is an early opportunity for its international debut.

Conclusions

Aquino has left the new President, Rodrigo Duterte, an interesting 'welcome' present, as politicians so often like to bequeath to their successors. President Duterte's track record of liking death squads and misogyny makes it seem unlikely that he would welcome a potentially independent privacy investigative body, or decide to give it generous funding.

For businesses that have become used to ignoring the Philippines' Data Privacy Act, including parties to outsourcing to the Philippines, it is time to pay the Act more attention, particularly once the IRRs become available. The meanings of many provisions in the Act are uncertain, including those concerning its "outsourcing exemption" mainly due to poor drafting.[8] The National Privacy Commission does have considerable powers, so care is needed until some of the uncertainties are resolved.

REFERENCES

1 Details of appointees mainly from Baker & McKenzie 'President appoints Philippines' first set of privacy commissioners' Legal Bytes (undated) www.lexology.com/library/document.ashx?g=3955c3db-b6a9-4f82-81d5-c17ff0f6bf78

2 Newsbytes Philippines 'DOST exec named first commissioner of National Privacy Commission' 7 March 2016 http://newsbytes.ph/2016/03/07/dost-exec-named-first-commissioner-of-national-privacy-commission/

3 ABS-CBN News 'Nat'l Privacy Commission probes Comelec hacking', 29 Apr 2016 http://news.abs-cbn.com/halalan2016/nation/04/29/16/natl-privacy-commission-probes-comelec-hacking

4 James Temperton 'The Philippines election hack is 'freaking huge' *Wired UK*, 14 April 2016 <http://www.wired.co.uk/news/archive/2016-04/14/philippines-data-breach-fingerprint-data/viewgallery/627935>

5 Ghio Ong 'IT grad, 23, arrested for Comelec website hack' *The Philippine Star* 22 April 2016 www.philstar.com/headlines/2016/04/22/1575594/it-grad-23-arrested-comelec-website-hack

6 Baker & McKenzie 'President appoints Philippines' first set of privacy commissioners' Legal Bytes (undated) www.lexology.com/library/document.ashx?g=3955c3db-b6a9-4f82-81d5-c17ff0f6bf78

7 For details of this and other aspects of enforcement powers, see G Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014), pp. 348-352.

8 See generally Greenleaf *Asian Data Privacy Laws*, Chapter 12 'The Philippines and Thailand: ASEAN's Incomplete Comprehensive Laws'.

Consumer law strengthens data protection rights in Germany

Consumer organisations have a role to play, just like in the forthcoming GDPR. **Irene Kamara** and **Paul De Hert** explain.

On 24 February 2016 Germany's "Act to Improve the Civil Enforcement of Consumer Protection Provisions of Data Protection Law" entered into force (hereafter Civil Enforcement Act).[1] The new law (art.3),[2] which amends Germany's Act on Injunction Relief (Gesetz über Unterlassungsklagen – 'UKlaG'),[3] extends among others the powers of consumer protection and other associations to bring claims in court relating to the collection and processing of consumer personal data.

'Consumer protection law' to include DP rules

The new act (Art. 3 § 1 (c) (cc)) broadens the definition of 'consumer protection laws' to include rules governing:

a) the collection of personal data of a consumer by an enterprise;
b) the processing or use of personal data collected about a consumer by an enterprise.

Such personal data rules fall within the scope of the amended provision when collected for purposes of advertising, market and public opinion research, creation of personality and usage profiles, trade of addresses or of other data, or other similar commercial purposes.

Noteworthy is the phrase "other similar commercial purposes", which renders the applicability of the provision particularly broad, as meaning the collection, processing and use of consumer personal data for practically any commercial purpose. The only explicit limitation to the phrase "other similar commercial purposes" is provided in Art. 3 § 1 (c) (dd)) which refers to the cases of consumer personal data being collected, processed or used by an enterprise exclusively for the establishment, implementation or termination of a legal transaction with the consumer.

Consumer associations and the role of DPAs

Not-for-profit consumer associations can now bring actions in civil law courts on behalf of consumers in order to cease and prohibit future violations of data protection laws in Germany. This is made possible for the cases of wrongful collection, processing or use of consumer's personal data by an enterprise falling within the scope of the "consumer protection laws", as described above. Consumer associations, including those qualified under Directive 2009/22/EC,[4] can act either on their own initiative or at the request of consumers.[5] These associations have the right to send the relevant enterprise a warning letter ('Abmahnung') or file for an injunction suit against the enterprise alleged to be violating the data protection laws.

The new act also reserves a role for the Data Protection Authorities (DPAs): the court is required to listen to the competent domestic DPA before making a decision relating to the claim.

> It is remarkable that the claims related to the data protection violations do not lead to an award of damages.

Even though this is a civil law procedure, one cannot but agree with involving the DPA as the competent authority to express an expert opinion on data protection related claims. The presence of the DPA in such hearings can bring in additional expertise and may provide guarantees for uniform application of the data protection law in Germany.[6]

Impact on consumers and enterprises

It is remarkable that the claims related to the data protection violations, according to the new Civil Enforcement Act, do not lead to an award of damages. The non-compliance with the court order however, if the injunction suit is successful, may lead to pecuniary penalties. In general, an injunction as a judicial remedy has the characteristic of being a fast procedure, aiming to prevent or cease a wrongful activity. In the data protection cases under the new act, a granted injunction would mean that the enterprise needs to comply immediately with the court order. Hence this is a fast and direct enforcement of the data protection rules. For the consumer, who often does not have the financial means to pursue his or her rights in court, a provision allowing a consumer protection association to act on his or her behalf facilitates the exercise of his/her data protection rights. These amendments to the Injunctions Act (UKlaG) have therefore long been advocated by consumer associations, who could formerly bring actions to court related to data protection only if the actions concerned violations of terms and conditions[7].

Compatibility with the GDPR

The General Data Protection Regulation 679/2016 (GDPR),[8] which entered into force in May 2016 and applies from 2018 onwards, establishes remedies for data subjects in Art. 77 to 79. These articles concern the right of the data subject to lodge a complaint with the supervisory authority, the right to an effective judicial remedy against a supervisory authority and the right to an effective judicial remedy against a controller or processor. Art. 80 of the GDPR provides the data subject with the right to mandate an organisation to exercise certain rights on his or her behalf. According to Art. 80§1, the

mandated body, association or organisation should be not-for-profit, established in accordance with the national legislation of the Member State, serve public interest objectives and be active in the field of data protection. The organisation may be mandated to lodge a complaint on behalf of the data subject, to exercise the rights of Art. 77-79 and to exercise the right to receive compensation (Art. 82) on data subject's behalf.

The rationale of the new German consumer act is in line with Art. 80 GDPR: representation of data subjects by not-for-profit bodies in exercising certain data protection rights. Although Art. 80 GDPR has a broader scope than Art. 3 of the new German consumer law, which is limited to injunction relief, consumer data and the German jurisdiction, Art. 80 GDPR provides the legal basis for the German law at EU level.

Conclusion

The new Civil Enforcement Act shows how consumer law remedies can be used to enforce data protection legislation.[9] Although fragmented at EU level, consumer protection law has tools and mechanisms in place, unknown to data protection law, which can help to guarantee data protection rights understood as consumer rights. These include monitoring tools, consumer awareness mechanisms and tools for enforcement and redress.[10] It remains to be seen how the act will work in practice: whether the consumer associations will make use of their new capacities,[11] how the enterprises will respond to cease-and-desist letters and injunctions suits regarding data protection laws.

AUTHORS

Irene Kamara is attorney-at-law and doctoral researcher at the Law, Science, Technology and Society (LSTS) Research Group of the Vrije Universiteit Brussel. Paul de Hert is professor at the Vrije Universiteit Brussel and the University of Tilburg.

INFORMATION

Information: The authors would like to thank Robert Benditz for his assistance at the research stage of drafting this contribution. Any mistakes are the authors' alone.

REFERENCES

1 *PL&B International,* April 2016, p.15 'German consumer law creates new DP rights'.
2 Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts Vom 17. Februar 2016, available http://tinyurl.com/jtl3tbj
3 Unterlassungsklagengesetz in der Fassung der Bekanntmachung vom 27. August 2002 (BGBl. I S. 3422, 4346) (last amended with Artikel 3 des Gesetzes vom 11. April 2016 (BGBl. I S. 720)), available www.gesetze-im-internet.de/uklag/BJNR317300001.html
4 European Parliament and Council, Directive 2009/22/EC of the European Parliament and of the council of 23 April 2009 on injunctions for the protection of consumers' interests, OJ L 110/30, 1.5.2009 .
5 Fabian Niemann, Lennart Schüßler, 'Germany: New Right of Action for Consumer and Competition Associations Increases Risk of Data Protection Violations', 24 February 2016, available www.twobirds.com/en/news/articles/2016/global/neues-klagerecht-fur-verbraucher-und-wettbewerbsverbande
6 Andreas Fillmann and Annette Demmel, Germany's step to enhance data protection rights of its citizens "Act to improve the civil enforcement of consumer protection provisions of data protection law", *Lexology*, 10 February 2016.
7 See press release of the German Consumer Protection Association of Verbraucherzentrale Bundesverband e.V , 17 December 2015, available http://www.vzbv.de/pressemitteilung/datenschutz-endlich-besser-durchsetzen
8 European Parliament and the Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, 4 May 2016.
9 Administrative and criminal remedies are also used for the enforcement of the right to personal data protection. See Paul De Hert, Gertjan Boulet, 'The Co-existence of Administrative and Criminal Law Approaches to Data Protection Wrongs' in David Wright and Paul De Hert (eds.) *Enforcing Privacy*, Springer 2016, p. 357f.
10 Jana Valant, 'Consumer Protection in the EU. Policy review', European Parliamentary Research Service, September 2015, p.5f.
11 In other national jurisdictions, such as Norway for instance, consumer associations are active in the data protection field. The Norwegian Consumer Council has started a campaign against apps that breach data protection legislation. See Norwegian Consumer Council, 'Runkeeper tracks users when the app is not in use', 13 May 2016, available http://www.forbrukerradet.no/side/runkeeper-tracks-users-when-the-app-is-not-in-use/

EU Cyber Security Directive in force in August

The European Union is preparing to have the Network and Information Security (NIS) Directive (Cyber Security Directive) in force from August 2016.

The EU Presidency has announced that the Council adopted its position at its first reading on 17 May. The Council will transmit its position to the European Parliament, which is expected to vote during its plenary session in early July. This would allow the Directive to enter into force in August.

EU Member States will then have 21 months to implement the Directive into national law. The European Commission has already been making necessary steps to prepare the ground for the Directive's implementation, the Presidency says.

- *See PL&B International, issue 139, February 2016, for a detailed analysis of this Directive's provisions.*
- *See the Presidency's note at http://data.consilium.europa.eu/doc/document/ST-8896-2016-INIT/en/pdf*

Vietnam's cyber-security law strengthens privacy… a bit

The law is limited to commercial processing of personal information in cyberspace. **Christian Schaefer** and **Graham Greenleaf** report.

Vietnam's new Law on Cyber-Information Security, enacted in November 2015,[1] comes into effect on 1 July 2016 (the "Law"). As a law enacted by the National Assembly, it is the second highest form of legislation in Vietnam, superseded only by Vietnam's Constitution and international treaties.2 This article assesses whether the Law's scope, and the data privacy principles it sets out, significantly expand Vietnam's existing data privacy laws, which to date are, in a piece meal manner, scattered across various regulations that apply to the IT, telecommunications, banking, e-commerce and consumer privacy sectors.[3] Section references are to the Law except where noted.

Clearer concept

The Law provides clearer concepts of personal information and processing, but with a focus limited to commercial processing and only in cyberspace. It offers two useful definitions for personal information and data processing. It provides that "[p]ersonal information means information associated with the identification of a specific person" (Art. 3(15)) and "[o]wner of personal information means a person identified based on such information" (Art. 3(16)). This is a broader definition of "personal information", especially when compared to existing definitions in Decree 72/2013/ND-CP on the Management of Internet Use where "personal information" is defined as "information which is attached to the identification of the identity and personal details of an individual including name, age, address, people's identity card number, telephone number, email address and other information as stipulated by law" (Article 3(15) of Decree 72) or Decree 52/2013/ND-CP on E-commerce where personal information is defined as "information contributing to identifying a particular individual, including his/her name, age, home address, phone number, medical information, account number, information on personal payment transactions and other information that the individual wishes to keep confidential." (Article 3 of Decree 52). The broader scope of the definition is significant as the Law spells out prohibited acts in relation to processing personal information.

Furthermore, and unlike the Law on Information Technology which does not define "processing" of personal information, the Law now defines "[p]rocessing of personal information" as "the performance of one or some operations of collecting, editing, utilizing, storing, providing, sharing or spreading personal information in cyberspace for commercial purposes" (Art. 3(17)). Articles 17 to 19 of the Law then provide comprehensive regulations on the requirement of how personal information must be managed. However, the definition at the same time limits the scope solely to "organisations and individuals processing personal information" in a commercial context and does not apply to the processing of personal information for government or non-commercial purposes. In addition, given the overall ambit of the Law, the Law imposes these requirements only to processing of personal information in cyberspace.

The law is unusual in that it defines "cyberspace" to mean "an environment where information is provided, transmitted, collected, processed, stored and exchanged over telecommunications networks and computer networks" (Art. 3(2)). This suggests that the scope also includes VPNs and possibly certain intranets. "Information system means a combination of hardware, software and databases established to serve the creation, provision, transmission, collection, processing, storage and exchange of information on the network" (Art. 3(3)), and the scope of the Law is thus limited to cyber-information security activities on such a network.

Cyber-security with a privacy balance

"Cyber-information security means the protection of information and information systems in cyberspace from being illegally accessed, utilized, disclosed, interrupted, altered or sabotaged in order to ensure the integrity, confidentiality and usability of information" (Art. 3(1)). Article 4 sets out the general obligations of organisations (private and public sector) and individuals to ensure this cyber-security, but also requires that "[t]he response to cyber-information security incidents must guarantee lawful rights and interests of organizations and individuals and may not infringe upon privacy, personal and family secrets of individuals and private information of organizations" (Art. 4(3)). Security should therefore not trump privacy.

A code for data privacy in cyberspace

Within this limited scope, Chapter II Section 2 of the Law sets out what is probably the most comprehensive set of data privacy principles yet found in a Vietnamese law (Arts. 16-19). Without significantly departing from previous laws, the following requirements imposed on organisations and individuals that process personal information within a commercial context are more precise:

- **Consent requirements** – "Collect personal information only after obtaining the consent of its owners regarding the scope and purpose of collection and use of such information" (Art .17(1) (a)).
- **Use limitation** – "Use the collected personal information for purposes other than the initial one only after

obtaining the consent of its owners" (Art. 17(1) (b)).

- **Disclosure limitation** – "Refrain from providing, sharing or spreading to a third party personal information they have collected, accessed or controlled, unless they obtain the consent of the owners of such personal information or at the request of competent state agencies" (Art. 17(1) (c)). The State need only "request", so there is no effective limitation on disclosure by state agencies.
- **Right of access** – "Owners of personal information may request [processors] to provide their personal information collected and stored by the latter" (Art. 17(3)).
- **Automatic deletion and notification** – "… shall delete the stored personal information when they have accomplished their use purposes or the storage time has expired and notify such to the owners of such personal information, unless otherwise prescribed by law" (Art. 18(3)).
- **Publication of protection measures** – "…shall develop and publish their own measures to process and protect personal information" (Art.16(3)).

Enforcement

"Prohibited acts" in cyberspace include not only spreading spam or malware but also "[i]llegally collecting, utilizing, spreading or trading in personal information of others; abusing weaknesses of information systems to collect or exploit personal information" (Art. 7(5)) which is broader in scope and encompasses illegal acts of third parties more comprehensively than the prohibited acts set out currently in the Law on Information and Technology. Moreover, hacking "information on clients that lawfully use civil cryptographic products" (Art. 7(6)) is prohibited. But "using or trading in civil cryptographic products of unclear origin" is also prohibited (Art. 7(6)), so privacy protection via cryptography is of limited legality in Vietnam. Trading in "civil cryptographic products and services" must be licenced (Chapter III, Civil Cryptography), and can be suspended at the request of state agencies (Art. 35(6)).

"Individuals violating this Law shall, depending on the nature and severity of their violations, be disciplined, administratively sanctioned or examined for penal liability and, if causing damage, pay compensation in accordance with law" (Art. 8). Unlike the Law on Information and Technology that sets out different consequences for violations by individuals and organisations, it is unclear what the sanctions for the violations committed by organisations are under the Law until implementing regulations provide more details on consequences for violations by organisations.

Article 20 requires only "state management agencies" to "establish online information channels for receiving petitions and reports from the public" and to "annually inspect and examine personal information-processing organizations and individuals; to conduct extraordinary inspection and examination when necessary". It would seem that they are then able to take enforcement steps under Article 8.

The Ministry of Information and Communications has the most general responsibility for implementation of the Law (Art. 52(2)), including "[t]o conduct examinations and inspections, settle complaints and denunciations, and handle violations of the law", but other specified Ministries also have significant responsibilities (Art. 52(2)(h)).

Conclusion: Another sectoral law for Vietnam

From a privacy perspective, this law is therefore limited to "commercial processing of personal information in cyberspace". The existing Vietnamese data privacy laws are sectoral laws, and the Law has not introduced any major changes to the existing regulations. However, the content of the data privacy protections is generally more precise and stronger. It is to be seen whether the implementing regulations of the Law will provide any further development. So far, it is another small step forward.

AUTHORS

Authors: Christian Schaefer is Managing Partner at Asia Counsel, Ho Chi Minh City.
Email: christian@asia-counsel.com
Graham Greenleaf is Asia-Pacific Editor for *PL&B International*.

REFERENCES

1 Law on Cyberinformation Security, National Assembly, No. 86/2015/QH13, November 19, 2015.
2 G Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014), p. 363.
3 Greenleaf *Asian Data Privacy Laws* Chapter 13 'Vietnam and Indonesia – ASEAN's Sectoral Laws'.

UN Special Rapporteur on Privacy finds resources for his job

At the ASSO DPO conference in Italy, Dr Joseph Cannataci, United Nations Special Rapporteur on the Right to Privacy, told *PL&B* that although he receives a low official budget, he is finding resources to do this job. **Stewart Dresner** reports from Milan.

The United Nations Special Rapporteur on the Right to Privacy, Dr Joseph Cannataci, has told *PL&B* that, although he receives no personal remuneration for his UN work – and he is only allocated a small UN budget for travel (two country visits and two conferences per year) – he has recently been allocated a budget for staff which should enable the UN to recruit three or four staff members to work on his mandate.

The funds were approved in January 2016, almost six months after his mandate commenced and to date he has had to make do with the services (interrupted for one month) of one single UN Human Rights Officer recruited on a temporary contract. The UN recruitment systems work so slowly that even though 25% of his three year mandate is already over the staff recruitment procedure for his mandate has not yet been completed and he has again recently asked the senior officials concerned to expedite matters. (See also *PL&B International* April 2016 pp.10-12).

In spite of these teething troubles – some of which are understandable given that the mandate of the Special Rapporteur for Privacy (SRP) is a completely new one and therefore things had to be set up from scratch – in point of fact the SRP has somehow still found the resources to do his job. Helped by a long experience in finding resources and managing privacy projects since 1984, he utilises and builds on his existing contacts, and is grateful to those colleagues and friends who have often volunteered their own personal time in an effort to help him to get things going.

He is especially indebted to the 10-person team at the Department of Information Policy & Governance which he heads at the University of Malta and the 22 colleagues from STeP, the Security, Technology & e-Privacy Research Group which he co-founded and co-directs at the University of Groningen in the Netherlands.

Over the past eight years alone he has co-designed and won over €30 million of funding for privacy-related collaborative research projects, mostly from the European Commission. More than 170 researchers from over 25 countries around the world have been involved or are still involved in these projects and many of them continue to contribute to his efforts in various ways. So his mood is up-beat and, as a keen lover of music, he described his current position in Beatlespeak as a combination of "We can work it out" and "I get by with a little help from my friends".

Professor Cannataci's main concern now is to convert the initial enthusiasm with which he has been welcomed into something far better resourced and sustainable in both the mid and long term. Apart from impact on substantive issues, he also wishes his legacy as SRP to be a sustainable project with capable people and sufficient resources. As an example of the need for resources to continuously monitor new privacy infringements and proposed legislation, he drew attention to the challenges to privacy from government initiatives in the past six months in Austria, Brazil, China, France, Germany, Russia, the UK and the US to mention but a few of the countries where his mandate is monitoring developments on a day-to-day basis.

He is now seeking more funding and capable people, especially domain-specialists, to be seconded from or funded by non-governmental organisations, Data Protection Authorities and companies. His only condition for accepting resources is that there must be no strings attached. He will accept help only if he can use the resources with complete independence.

Although privacy is not defined in Art. 12 of the UN Declaration of Human Rights (he said that it is the most translated document in the world), this apparent weakness also gives him some flexibility in his work. Clearly, in historical terms, the EU has taken the lead and, having in April adopted the EU General Data Protection Regulation (GDPR), is influential across the world for companies wanting to do business in this region of 500+ million people.

On the other hand, there are more than 100 countries world-wide which have already introduced some form of privacy legislation and the harmonisation and improvement of global standards in privacy safeguards and remedies remains a huge task for decades to come. Over and above the effort dedicated to improve safeguards and harmonisation, the SRP is also committed to working towards privacy protection being introduced and strengthened in all the 190+ member states of the UN.

He already has trips planned to Africa, America (north and south), Asia and Australia with Europe continuing to be another key player in various privacy initiatives. PL&B met Cannataci in Milan Italy, as he was *en route* to a speaking engagement in New York at the end of April. His subsequent trips included visits to Privacy Week in New Zealand and Privacy Awareness week in Australia during May, then keynote speeches in Washington DC, Copenhagen and Strasbourg in June and back in New York in July. "...and that's only the first half of 2016, all activities resourced from external funding and not the UN," he smiles. The second half of 2016 promises to be at least as busy, and Cannataci will speak at *PL&B's* 30th Anniversary International Conference, 3-5 July 2017.

INFORMATION

Professor Dr. Joseph A. Cannataci is Chair in European Information Policy & Technology Law, Department of European & Economic Law, University of Groningen, The Netherlands
www.rug.nl/staff/j.a.cannataci/

book review

Privacy in the modern age: The Search for Solutions
Edited by Marc Rotenberg, Julia Horwitz, and Jeramie Scott

This book is a compilation of 24 articles all looking at different privacy issues. The first one is by the book's editor, Marc Rotenberg, President of the US-based Electronic Privacy Information Center (EPIC). He looks back on EPIC's first 20 years. A main player in the US privacy debate, EPIC has contributed much not just in the field of data protection but also freedom of information. The book reminds us of the interesting fact that EPIC was instrumental in making the Federal Trade Commission take a stand on privacy. "In some respects the outcomes were better than we anticipated," Rotenberg writes. "The Federal Trade Commission would often take the core of an EPIC complaint and then find other practices we had missed. The remedies proposed were typically more sweeping than we had recommended. Once a consent order was in place, the agency would maintain oversight of the company's practices for twenty years."

The contributors to this book offer solutions to modern-day privacy problems. The articles, too many to review in this space, vary from the future of heath privacy to NSA surveillance, and from robots and drones to user adoption of privacy technologies. A particularly useful article for privacy practitioners engaged in big data processing is 'Envisioning privacy in the world of big data' by Christopher Wolf, director of the Privacy and Information Management Practice at Hogan Lovells US LLP. Wolf says that while companies cannot provide notice for a purpose that is yet to exist, nor can consumers provide informed consent for an unknown use of their data, context is the important issue. "Often, context is understood to mean that personal information should be used only in ways that individuals would expect, given the context in which information was disclosed and collected. However, there are uses of data that may be outside individual expectations but have high societal value and minimal privacy impact that should be encouraged. More work is needed to define and frame context."

Reviewed by Laura Linkomies

Published in April 2015 by The New Press, New York. ISBN 978-1-62097-107-9 (hard cover $25.95) 272 pages
ISBN 978-1-62097-108-6 (e-book)

Dynamic IP addresses can be personal data, Court of Justice of the European Union says

The Advocate General of the Court of Justice of the European Union (CJEU) has issued an opinion on 12 May in the case *Patrick Breyer v. Federal Republic of Germany* which suggests that dynamic Internet Protocol (IP) addresses fall within the EU Data Protection Directive. The case is about whether the Federal Republic of Germany may save the IP addresses of visitors to its websites. The essential question is whether the Data Protection Directive should be interpreted to mean that an IP address stored, in connection with a visit to a website, will constitute personal data if a third party has additional data which will make it possible to re-identify the individual.

The Advocate General of the CJEU says that if dynamic IP addresses were not regarded as personal data from the point of view of the operator of an Internet service, they could retain them indefinitely and at any time ask the Internet Service Provider (usually phone companies) for additional data in order to combine them with the dynamic IP address.

The court is yet to give its final decision, but often the Advocate General's view is followed. The German government's view was that the IP addresses would not be personal data. The European Commission pointed out that retaining IP addresses and the additional information may make identification possible in case of an attack against the network – a purpose IP addresses are retained for in the first place.

"If followed by the Court of Justice, the Opinion will have broad implications for EU data protection law, even the forthcoming General Data Protection Regulation (the GDPR). In particular, the Opinion will be relevant for any industries that handle de-identified personal data, and re-confirms the limits that national legislators need to respect when deviating from EU-level data protection legislation," said Monika Kuschewsky of Covington LLP.

• *The English translation has not yet been published, as of 4 June, but several other language versions, including German, Spanish, French and Italian can be seen at http://tinyurl.com/hscfrwx*

EU Commission revisits e-privacy Directive

The European Commission launched, on 12 April, a public consultation on the revision of the e-Privacy Directive. It is expected that the Commission will issue a legislative proposal on e-privacy by the end of this year.

The Consultation consists of two parts. The first part gathers views on how the current e-privacy regime is working. The second half encourages organisations to submit their views on possible changes to the law.

The Commission says the following areas are of particular importance:

1. Ensuring consistency with the EU General Data Protection Regulation
2. Addressing inconsistencies in the current implementation of the e-privacy Directive
3. Taking into consideration new market and technological realities, such as the question of whether Voice over IP and instant messaging providers should be subject to e-Privacy requirements
4. Enhancing security and confidentiality of communications.

• *The consultation runs until 5 July 2016. See https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive*
The consultation document is available in French, English and German.

EU and US sign Umbrella Agreement for law enforcement data transfers

The EU and US Justice and Home Affairs Ministerial Meeting signed the so called Umbrella Agreement, which sets a standard for data transfers by law enforcement authorities. The EU and the US said they are committed to work together in the implementation of this agreement to ensure that it benefits both citizens and law enforcement cooperation. The next step will be to seek approval by the European Parliament.

The Umbrella agreement has been seen, from the EU's side, as an essential element for creating trust and finding a mechanism for data transfers in general. The EU's Commissioner responsible for data protection, Věra Jourová was present at the meeting, but no details were released about the state of play with the proposed EU-US Privacy Shield.

The parties also reaffirmed their commitment to closer cooperation, especially in the context of evolving and shared challenges that affect the security and rights of citizens on both sides of the Atlantic.

They also discussed information sharing in the context of security, on counterterrorism policies and terrorist financing, on money laundering, data protection and on practical cooperation to tackle transnational organised crime.

Part of the talks was a five-year review of the 2010 EU-US Mutual Legal Assistance Treaty, a key mechanism for transatlantic criminal justice cooperation. Facilitating access to electronic evidence is a particular concern of the review, and the participants committed themselves to improving their practices through which they obtain such evidence.

• *See the statement of 2 June at www.justice.gov/opa/pr/joint-eu-us-press-statement-following-eu-us-justice-and-home-affairs-ministerial-meeting#_ftn1*

UK Investigatory Powers Bill moves to Lords

The legislative process on the Investigatory Powers Bill came to an end in the House of Commons on 7 June and the Bill moved to the House of Lords, where the first reading took place yesterday. The second reading – and the general debate on all aspects of the Bill – takes place on 27 June.

Anne McLaughlin, MP for the Scottish National Party said:

"I understand that the Government are arguing that new clause 5 is a privacy clause, but how can we trust their commitment to privacy when between the publication of the draft Bill and the publication of this Bill the significant change to deal with the need for privacy to be of primary importance entailed simply changing the name of part 1 from "General Protections" to "General Privacy Protections"? This is not about words, but about intent, action and commitment, and inserting one word appeases no-one."

The Scottish National Party, the Green Party, and the Liberal Democrats opposed the Bill's third reading with 69 votes.

The Bill's bulk collection powers will now be subject to an independent review by the government's reviewer of anti-terrorism legislation, David Anderson Q.C. Results are expected in the summer.

• *The Bill, as introduced in the House of Lords on 8 June, www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf*
The review's terms of reference: https://terrorismlegislationreviewer.independent.gov.uk/bulk-powers-review/

Finland: Employer may not access an ex-employee's emails

The Turku Court of Appeal has ruled on an employer's right to retrieve and open an employee's work-related emails after the employee has resigned. The Court found that by forwarding e-mails from the employee's work account to their own accounts without complying with the statutory procedural provisions, the employer's representatives had violated the of Act on the Protection of Privacy in Working Life (759/2004, as amended), law firm Roschier reports.

The employer did not try to retrieve or open the employee's private e-mails. However, explicit consent should have been sought for accessing the work email, the court said.

"In this case, the employee had agreed in an e-mail that for a period of nine days the private messages sent to his work account would be forwarded to his personal e-mail address. However, as the explicit consent to access his work account was restricted to a period of nine days following his resignation, the e-mail could not be regarded as permission to still access his account several months later. The Court also found that in this case the employer's IT Policy did not include the employee's consent to examine or read his work e-mails in the event of resignation. The Court also held that in any event the mere reception of such document cannot constitute consent if the employee's familiarization with the terms and conditions is not confirmed in any way."

• *The judgement is not yet final. See http://bit.ly/1rOPeyO*

EDPS: Privacy Shield is not good enough

The European Data Protection Supervisor (EDPS) has issued an Opinion in which he says that the proposed EU-US Privacy Shield is not robust enough.

Giovanni Buttarelli, EDPS, said: "I appreciate the efforts made to develop a solution to replace Safe Harbor but the Privacy Shield as it stands is not robust enough to withstand future legal scrutiny before the Court [of Justice of the European Union]. Significant improvements are needed should the European Commission wish to adopt an adequacy decision, to respect the essence of key data protection principles with particular regard to necessity, proportionality and redress mechanisms. Moreover, it's time to develop a longer term solution in the transatlantic dialogue."

Recognising that organisations should not be expected to constantly change compliance models, the EDPS proposes some improvement to Privacy Shield. These include integrating all main data protection principles, limiting derogations and improving redress and oversight mechanisms.

It is expected that the Article 31 Group, consisting of EU Member States representatives, will form its view this summer. A positive decision would enable the EU Commission to adopt the adequacy decision for the Privacy Shield.

In the meantime in Germany, Hamburg's Data Protection Commissioner, Dr Johannes Caspar, has fined three companies that have been relying on Safe Harbor. According to Der Spiegel online, the three companies concerned are Adobe (fined €8,000), Punica (fined €9,000) and Unilever (fined €11,000). The maximum level of fines is €300,000, but all three companies have found a different legal basis for their international data transfers.

- *The EDPS Opinion, issued on 30 May, is available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf*
- *On the Hamburg decision, see (in German) http://www.spiegel.de/netzwelt/netzpolitik/safe-harbor-suender-hamburgs-oberster-datenschuetzer-verhaengt-bussgelder-a-1096091.html*

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

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

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

Included in your subscription:

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

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

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

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

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Chief Privacy Officer, BT Retail, UK**"

Subscription Fees

Single User Access

International Edition **£500 + VAT***

UK Edition **£400 + VAT***

UK & International Combined Edition **£800 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

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

Subscription Discounts

Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.

Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

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

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK