ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

GDPR – a useful tool and status changer for DPOs

Beverley Flynn reports on the changing status of Data Protection Officers under the EU General Data Protection Regulation.

The EU General Data Protection Regulation (GDPR) is coming to the UK and, with it, the requirement for public authorities and certain other organisations (whether data controllers or data processors) to appoint a data protection officer (DPO) to assist with compliance. Although the use of DPOs is established in certain jurisdictions, the mandatory DPO model is new for the UK.

Whilst some UK organisations have had an in-house voluntary DPO function for some time, the concept of a mandatory officer will

Continued on p.3

Companies prepare for new regime as GDPR beckons

Organisations readiness varies and they cite the importance of top-level support. **Laura Linkomies** reports.

A *PL&B* roundtable facilitated the exchange of ideas and experience on GDPR compliance and readiness. It was clear that while some organisations are quite advanced in their preparations, others have focused only on certain areas and are waiting for more guidance from the ICO and the EU Article 29 DP Working Party.

The first topic to be discussed was data mapping, which has been widely regarded as a tool to get ready for the GDPR's accountability requirement. While the general notification requirement has been abolished,

Continued on p.5

Search by key word on
www.privacylaws.com

Subscribers to paper and electronic editions can access the following:

- Back Issues since 2000
- Special Reports
- Materials from PL&B events
- Videos and audio recordings

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

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

Issue 89 **January 2017**

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

DPOs ... from p.1

be new particularly for small and medium-sized businesses. Businesses that need a mandatory DPO will need to ensure that any existing DPO role is in line with the GDPR requirements. The distinction between a mandatory or voluntary DPO may also mean that it takes some time for the industry to embed these changes and appreciate the value and advantages of each role. In addition, there is potential for more widespread use of external DPOs (either individual consultants or organisations) – again, a concept already used in other jurisdictions.

The recent EU Article 29 Data Protection Working Party guidance entitled "Guidelines on Data Protection Officers" (Article 29 Guidance) gives some further granularity to the position. The Article 29 Guidance reflects the move towards an accountability-based compliance framework and specifically states that DPOs will be at the heart of the new legal framework and facilitate compliance. So how might the GDPR affect the role of DPO?

GDPR requirement – voluntary or mandatory?

Data controllers and data processors must appoint a mandatory DPO in any case where:

1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
2. the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
3. the core activities of the data controller or data processor consist of processing on a large scale of special categories of data (i.e. sensitive personal data) or personal data relating to criminal convictions and offences.

UK legislation could also require organisations to appoint a DPO in other circumstances.

The Article 29 Guidance helps clarify the meaning of "core activities", "regular and systematic monitoring" and "large scale" which is useful. Core activities are considered to be operations necessary to achieve the data controller or data processor's goals. For example: in the case of a hospital, processing health records for patients' healthcare would count as a core activity. For a security company carrying out surveillance on behalf of shopping centres, the surveillance would be a core activity. Ancillary support functions necessary or essential to an organisation simply to support the core activity of the business itself would not normally be considered core, for example, payroll and IT support. At this stage, the Article 29 Guidance does not give precise numbers but does give some helpful examples of what might be considered "large scale". This includes the tracking of data subjects via travel cards, the processing of geo-location data of an international fast food franchise's customers for statistical purposes by a data processor specialising in that service and the processing of personal data for behavioural advertising by a search engine.

The first step for in-house DPOs will be to decide whether the mandatory DPO requirement applies, or whether the DPO has the option of retaining a voluntary status. The Article 29 Guidance makes clear that where a data controller is required to appoint a mandatory DPO, it does not follow that the data processor is also required to do so. In practice, it may be that more data processors may be required to appoint mandatory DPOs if they specialise in large-scale data management. For the first time, processors will be directly affected by the legal requirements.

Even if the mandatory requirement does not apply, the Article 29 Guidance positively encourages the voluntary appointment of DPOs. The interesting aspect for those sitting as voluntary DPOs is the extent to which the GDPR requirements can or do apply and will impact on their role.

Budget and funding – a useful tool

The GDPR may well be a useful tool, as it includes various legal mechanisms to preserve the DPO's independence and efficacy. In particular, organisations will need to ensure that:

1. their DPO is provided with the necessary resources and access for the DPO to perform tasks and maintain knowledge (this may involve training);
2. the DPO reports to the highest management level of the organisation;
3. DPOs are not given instructions regarding the exercise of their tasks and can act in an independent manner;
4. DPOs are not dismissed or penalised simply for performing their tasks; and
5. there is no conflict of interest with the DPO's other duties.

Failure to observe the rules in relation to DPOs could attract fines of up to €10 million or 2% of worldwide annual turnover, whichever is higher. This may be a useful tool in the armoury of those DPOs that are seeking to secure budget, implement projects, obtain resources and looking to fulfil ongoing training needs.

Senior management buy-in

A possible frustration for those nominally in charge of data protection can be a lack of resources or a senior sponsor. The GDPR introduces the concept of a mandatory DPO positon, thus securing the legitimacy of the role and adding further gravitas. The GDPR text together with the Article 29 Guidance also provides useful further written detail, which DPOs can point to in order to ensure that they:

1. are invited to participate regularly in both senior and middle management meetings;
2. are present when decisions affecting data protection implications are made;
3. are someone whose opinion carries weight, and if their advice is not followed, relevant parties document the reasons for not following it;
4. are promptly consulted in the case of a breach;
5. are actively supported by senior management possibly at board level;
6. have sufficient time to devote to their activities particularly in shared roles;
7. are given adequate financial

resources and infrastructure;
8. have their official designation communicated to the organisation;
9. have access to continuous training; and
10. are given access to support within the organisation.

DPO personal liability

There has been some concern that the DPO may be personally responsible for non-compliance with the GDPR. The Article 29 Guidance makes clear that mandatory DPOs are not personally liable and that it is still the data controller or data processor that bears the ultimate risk.

Who can be a DPO?

Appointing an external DPO: Whilst the current trend of many organisations is to appoint one internally, choosing the external DPO model can also be an option when managed carefully. The external provider may be either an individual consultant or an organisation. However, they must have sufficient levels of (i) expertise and (ii) professional qualities, with knowledge of both the business sector and the relevant organisation to enable them to fulfil their role. External DPO's may be a useful resource for small to medium-sized entities, where the use of data protection officers has not been addressed, or so far been allocated on a nominal basis.

Shared and single DPOs: A group of undertakings/companies can appoint a single DPO so long as the DPO is easily accessible from each establishment, i.e. the DPO is accessible by data subjects, the Supervisory Authority and internally to the organisation as a whole. Being able to communicate in the language of the designated Supervisory Authority and the data subjects will be helpful here. A DPO can then make use of others within the organisation or have a team. Note, in the case of a team, there can be certain requirements to give details of the DPO. For example, there is a general requirement to publish the contact details of the DPO (which need not include a specific name). However, in the case of a breach, the name of the DPO must be given to the Supervisory Authority.

Educational qualifications: There are no specific educational requirements, but the DPO must be able to fulfil the criteria set out below. For existing DPOs in their jurisdiction and existing organisation, this is unlikely to be an issue.

Expertise: The level of expertise must be commensurate with the nature and sensitivity of the personal data. For example, if the processing involves sensitive personal data or systematic transfers outside the EEA, this would need to be taken into account.

Professional qualifications: Although no specific exam or certification requirements are currently specified, it is relevant that the DPO has expertise in national and European data protection laws and an understanding of the GDPR. This is in addition to the knowledge of the business sector and the organisation itself.

Ability to fulfil tasks: Although a given in most job descriptions, this is understood to mean having the requisite personal qualities and also having the ability and position within the organisation.

Conflicts of interest: It is also a requirement that the DPO fulfils its tasks so as not to result in a conflict of interest. This means the DPO must be able to act in an independent manner, although this in itself does not necessarily prevent a team approach. The DPO may have other roles in the organisation provided it does not lead to such a conflict. Notably, the Article 29 Guidance specifically suggests that DPOs should not hold a position which could lead them to determine the purpose and means for processing personal data. As a rule of thumb, the Article 29 Guidance suggests that senior management positions such as Chief Operating Officer, Chief Financial Officer or Head of Marketing or HR or IT may give rise to conflicts of interest, but this is dependent on the organisational structure.

Enhanced rights against dismissal: Once the GDPR comes into effect, mandatory DPOs will have enhanced rights against dismissal and legal rights to access to resources and training. Therefore, it appears that the enhanced workload that the GDPR brings with it may not be without some benefits to DPOs.

The road ahead

Having personally experienced being in the position of both internal and external Data Protection Officer, are there any benefits to a company in having an external DPO? Certainly cost-sharing can be a financial benefit which can bring with it greater efficiency and cost savings. The advantage that an external DPO can bring is an element of independence, which is a requirement being sought under the new regime to avoid the inevitable conflicts of interests which an internal appointee may face.

Under the new framework of the GDPR, DPOs must have sufficient knowledge of the business and may need to be involved at significant decision-making stages. This means that the logistics of a shared external DPO with sufficient knowledge of the business has the potential to be challenging. For example, all parties will need to be aware that the external DPO needs time to adjust to local company culture and its organisational structure. Ultimately the aim must be to encourage the business to facilitate the DPO's integration, and involve the DPO at all levels whether HR, sales, marketing or IT.

The road ahead is not likely to be an immediately straightforward one, but potentially there will be plenty of DPO roles in the workplace and market - and companies will quickly become accustomed to having a useful DPO to bring expertise and legal compliance to every aspect of their business.

AUTHOR

Beverley Flynn is head of Data Protection at law firm Stevens & Bolton LLP and has experience in-house as a data protection officer.

 © 2017 PRIVACY LAWS & BUSINESS

UNITED KINGDOM
report

ISSUE NO 89 **JANUARY 2017**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

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

CONTRIBUTORS

Beverley Flynn
Stevens & Bolton LLP

Brian Johnston
Bristows LLP

Nicola Fulford and Rebecca Michael
Kemp Little LLP

Rebecca Cousin and Cindy Knott
Slaughter and May LLP

Pulina Whitaker
Morgan Lewis & Bockius LLP

Chris Pounder
Amberhawk Training Ltd

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

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

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

ISSN 2047-1479

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

© 2017 Privacy Laws & Business

comment

Guidance emerges on GDPR but not on Brexit

The EU Art. 29 Data Protection Working Party issued guidance for comment last December on GDPR implementation on the right to data portability, Data Protection Officers, and on identifying a controller or processor's lead supervisory authority.

UK-based companies with international clients and associate companies are becoming increasingly busy preparing for the GDPR (p.1). But those UK-based companies whose data processing is limited to personal data of UK data subjects are still unclear about how the law will apply to them in the period after the UK leaves the European Union.

The reason is that there is no clarity yet as to what the UK future data protection framework will look like for organisations with operations wholly in the UK. The Information Commissioner, Elizabeth Denham, is nevertheless planning GDPR guidance on children's personal data and consent, and the ICO has updated its GDPR guidance on its website to reflect guidance from the EU Art. 29 Data Protection Working Party (p.13). She considers that Brexit should not mean Brexit for data protection, and has been advising the government accordingly. Matt Hancock, Data Protection Minister, has confirmed to Parliament that the GDPR will apply in the UK starting in May 2018, but is keen to make wide use of the derogations available (p.12). Consultations are promised on the main changes. We will alert you when details emerge.

In the meantime, companies are advised to put a DPO in place or appoint an external adviser (p.1). But what about the UK's EU adequacy (p.18)? Will the UK have to apply for such an assessment in the future and join the queue after Japan and South Korea? The new Investigatory Powers Act (p.16) may cause problems on that front due to the extensive surveillance powers it permits if necessary and proportionate.

Our knowledgeable UK correspondents bring you news, analysis and compliance tips regarding security aspects and liability for companies of the Internet of Things (p.9), data protection damages (p.7) and data breaches under the GDPR (p.14).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

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

Join the Privacy Laws & Business community

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

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

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

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

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

Included in your subscription:

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

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

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

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

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

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

To Subscribe: www.privacylaws.com/subscribe

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

Subscription Fees

Single User Access

UK Edition **£440 + VAT***

International Edition **£550 + VAT***

UK & International Combined Edition **£880 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-10 users. Enterprise licence for 11+ users.

Subscription Discounts

Introductory 50% discount. Use code HPSUB (first year only) for DPAs, public sector, charities, academic institutions and small and medium companies.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

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

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

Satisfaction Guarantee

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

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