The DPO 2025: Expectations and challenges ahead

Dr Guido Reinke, a data culture advocate and senior privacy professional at a consumer credit reporting agency, and **Alexander Dittel**, Partner in Technology at Wedlake Bell LLP discuss ten future trends.

Some technologies move gradually, others exponentially. This has a direct effect on corporate governance processes. Whatever the pace of technology, compliance roles such as that of the Data Protection Officer (DPO) must keep up. Today's role of the DPO was born with the General Data Protection Regulation (GDPR) in 2018. Whilst early entrants were much in demand and eased into the profession by setting up data protection compliance programmes, those entering the profession now can easily lose sleep over the complexity of evolving privacy issues, rules and solutions. The top job of the DPO is no longer immediately available without climbing the data privacy career ladder first. This is understandable as we observe a near exponential rise in the level of expectations placed on the DPO in terms of skill, knowledge and experience.

The need for project managers becomes essential in making sure that no small, yet essential, privacy action item is missed out from the busy project schedules. Nevertheless, most DPOs remain a "one-man band". The DPOs' cry for resources being ignored by so many organisations contrasts with some organisations' sophisticated and well-resourced collective "Office of the DPO". However, in the current economic climate, budgets will be slashed and DPOs must present measurable success to the board in order to justify expenditure.

What other challenges and compliance trends might affect the role of the DPO in the foreseeable future until 2025?

> The DPO will have to park commercial pragmatism and be prepared to raise questions of data ethics with the board.

Trend 1: More technology means more regulation

Machine learning, pattern recognition, increased interoperability of systems, edge computing [computing done at a location as close to the originating source as possible], decentralised solutions, privacy enhancing technologies, blockchain, contextual AI-enhanced observing of online behaviour and other technologies all sound familiar. Learning robots help clean around the office. The metaverse and Web 3.0 will allow people to experience and collaborate in ways never envisaged before.

However, the virtual space offers absolute freedom which can turn into absolute surveillance and control with the switch of a button. A brain implant allows humans to instruct their device. Biometric data offers a safer solution for access control. The integration of digital into human life will soon change to integrating human into the digital world. Fast-paced technological and societal advancements leave no room for compliance assessment fatigue.

While the pro-regulation versus pro-market debate goes on, Industry 4.0 – or the fourth industrial revolution – brings as many opportunities as risks. Countries with universal human rights must engage in legislative activism rather than waiting for things to go wrong, as technologies could affect our personal freedoms such as our right to privacy, due process and freedom of speech.

The European Union has traditionally been a leader in timely regulation of digital technologies. The GDPR and ePrivacy Regulation will soon be followed by the AI Act, the Digital Markets Act, Data Act and Data Governance Act. Their objective is protecting individuals from high-risk activities and data dominance and unlocking responsible innovation.

In contrast, the AI Bill in the US does not enjoy legal authority, as it is not a binding law. In addition to data protection law, protecting children and vulnerable individuals in the digital space will be ensured under Singapore's Online Safety law, while the draft UK Online Safety bill is currently in Parliament, and the EU Digital Services Act was adopted 4 October 2022.

State intervention in digital worlds is no longer reserved for repressive regimes. Renewed legislative efforts to ban end-to-end encryption create tensions between user desire for privacy, commercial goals, innovation and government's data access needs.

Understanding the law is critical for the DPO. The staggering number of new laws around the world, even if they are GDPR clones, will bring its challenges. Often the same text or a concept like "consent" could mean different things under local application and cultural nuances.

Trend 2: Compliance is a collective effort

The DPO will be glad to join forces with other experts in the organisation including information technologies, information security, product, data governance, compliance and legal. This is reinforced by the nature of the data privacy impact assessment (DPIA) which brings together all relevant stakeholders to reinforce compliance approaches. Needless to say, the DPO's command of legal issues, data rights and compliance practice must allow him or her to debate issues, suggest alternatives and assess the risk on the go. With more people involved, the

DPO must understand the office politics in order to secure buy-in for important privacy projects, which some still disregard as needless bureaucracy.

Trend 3: Complex regulatory messaging

As digitalisation cuts across all sectors, isolated and ill-informed regulatory action could cause significant economic harm and affect legal certainty. The UK's Digital Regulation Cooperation Forum is an example of the much-needed regulatory cooperation and restraint. On the international level, some countries impose data localisation rules and requirements for technology to uphold "mainstream value orientations" which may seem impossible to reconcile globally. Others rely on obscure data transfer rules to declare foreign technology unlawful, despite reasonable regional initiatives that seek a way forward such as the Global Cross-Border Privacy Rules Forum formed by some APEC members, and now expected to be widened to have global reach.

The DPO's ability to discuss business strategy will depend on their understanding of the cross-sectoral picture and local regulatory thinking, which can sometimes be challenging even for a country's native organisations. Solutions driven by trade will likely be temporary and the DPO must remain cognisant of the underlying cultural and policy clashes which are ready to erupt at any time. Adherence to common standards such as the ISO/IEC JTC 1/SC 42 about artificial intelligence can help bridge cultural differences and lead to safer technology, governance of people and business, and meet compliance requirements in preferred markets.

Trend 4: Building public trust

Privacy-friendly organisations will attract more users. As consumers are increasingly willing to give away their privacy in exchange for the comfort of services, public trust can only grow if organisations commit to transparency, user control and openness to public scrutiny.

However, regulatory enforcement action around the world has put potential harms of digital technologies in the spotlight. Regulators continue taking action against multinational companies even long after the breach of law was remedied. Amidst shocking headlines, public trust remains fragile and the DPO must understand these regional regulatory tendencies which sometimes may seem political.

Data breach class action led by law firms in pursuit of financial gains is another challenge. However, public interest is served by meaningful litigation such as *Lloyd v Google* which concerned the circumvention of user choices. Organisations should not try to hide their wrong but rather work with their users on how to improve things going forward. However, coming clean could remain a difficult decision, often contradicting short-term commercial goals.

Trend 5: Data ethics will reach where laws do not

As the debate about what is right or wrong in technology evolves, many organisations adopt a Data Ethics Policy. The debate is essential in influencing regulatory positions in areas where policy-makers are stuck due to lack of awareness or a lack of political consensus. As the capabilities of technology continue to impress us, the DPO will have to park commercial pragmatism and be prepared to raise questions of data ethics with the board.

As analytics methods evolve, the same dataset can reveal more about individuals over time. With the increasing risk of invisible processing and significant automated decisions about people to their detriment, fairness and data ethics serve as an obscure safety net. The DPO must have regard to societal moods in formulating global compliance solutions or risk being out of touch and lose users. In some cases, the developing view on privacy and right or wrong will often be found in debates outside of the mainstream media.

Trend 6: Whistleblowing set to continue

No doubt the sustainability of mankind will depend on our ability to harness data. However, even the data privacy laws are not the failsafe compliance framework that would fully protect the individual. Whistleblower laws protect those courageous individuals who decide to speak up against their organisation about any unlawful or unethical practices at the risk of banishment from their professional community and industry.

Whilst data rights such as those under the GDPR empower the individual, only privacy advocates have the determination to push the public debate, the regulators and the courts, and force a change in corporate practices. More than ever people understand that these issues affect our daily lives. Organisations including their DPOs can be almost certain that shady practices will come to light sooner or later.

Trend 7: A decentralised job market

The gig economy, the pandemic and technological advancements have set in motion an unstoppable trend of a less dependent (yet dependable), remote workforce which is high in demand. A decentralised workforce means serving numerous employers to satisfy their current business needs. Particularly, external DPOs can fill the gap for organisations that do not need a full-time DPO.

The trend which has already started in physical work, logistics, administration and other tasks could soon start reaching compliance and risk roles at a large scale. Particularly, if the recession puts a halt to further hiring, organisations could turn to contractors for pressing tasks. The future could bring more specialist data protection roles provided by a decentralised workforce.

Organisations will have to find effective ways to monitor and control access to their intellectual property, confidential information and data by a large number of high turnover remote workforce. The DPO will have to address the risks as background checking, profiling and biometric access controls become commonplace.

Trend 8: Machine v human

"Is there a business tool that meaningfully helps with your day-to-day compliance decisions?" Most DPOs today will answer "no". This is about to change. Today, large language models can generate text which increasingly sounds like a conversation with a human. The model could be trained to give fairly reliable advice

based on vast amount of compliance resources which the DPO never had time to read.

The ability to tailor, assess and predict will pave the way for more integration of automated decisions in the workforce. Compliance might soon drive itself like cars and the DPO will emerge as the manager and quality controller of these new compliance tools.

Can a service that was created in breach of the law or data ethics be safely adopted by an organisation? The DPO will have to act as a gatekeeper and assess the compliance of incoming services developed in jurisdictions lacking regulation.

Trend 9: DPO's experience and ongoing training

Despite the growing maturity and sophistication of the DPO profession, it remains difficult to keep up with the influx of new laws, technologies and solutions. DPOs will have to continue deepening the legal, technological and commercial aspects of their role. The DPO will likely require access to legal advice and memberships in professional industry associations which can prove invaluable for knowledge sharing.

The DPO must understand technological processes and their evolving nature. For example, by adjusting a technological solution, a service could entirely change its dataflows during its lifecycle. Staying on top of the underlying privacy implications will require the DPO to take time to understand all processes and technological trends.

Trend 10: Measuring outputs

With the unpredictable future of global economies, demonstrating value in compliance becomes important. While the cost of non-compliance will generally outweigh the cost of compliance, cost cutting could put the DPO in a bind. Particularly, the need for additional resources will have to be justified by deliverables, Key Performance Indicators and growth plans. On the other hand, regulators in the EU will not hesitate to punish organisations which failed to appoint or to provide appropriate resources to a DPO.

Nevertheless, without a stable chair at board level, the DPO might struggle to present constant evidence of compliance successes. Most importantly, the DPO's word must carry authority and the privacy processes must be mandatory within an organisation and cannot be circumvented at will.

The DPO needs to plug into everything the company does. The DPO will also have to formulate a privacy strategy and growth plan, such as achieving a certain level of public trust through increased transparency, streamlining assessments, setting up compliance monitoring programmes, banning certain services, or helping the organisation to attain a compliance certification. The DPO will have to understand the Public Relations implications of any public messaging.

Bringing value to the organisation should be expressed in a language the board will understand such as revenue numbers or saved costs by, for example, fending off a regulatory enquiry. Nevertheless, one should resist the temptation of focusing on activities which yield recognition while neglecting other important compliance tasks.

Conclusion

Over the last four years we observe an increasing demand for DPOs who find themselves in an increasingly specialist profession. The role of DPOs is subject to a near exponential change, with demands on their skills, technical expertise, commercial awareness, people skills and sensitivity to office politics. This trend is set to continue with the digitalisation of the world as we know it.

DPOs will likely be at the forefront of technological development and formulating the vital data ethics debate and practical compliance rules for organisations.

AUTHORS

Dr Guido Reinke is data culture advocate and senior privacy professional at a consumer credit reporting agency and Alexander Dittel is Partner in Technology at Wedlake Bell LLP.
Email: adittel@wedlakebell.com

INFORMATION

In this article the authors present their personal views and not those of their organisations.

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Identical BCR mechanisms sought in the UK and EU

A *PL&B* and Hogan Lovells Workshop identified differences between the current EU Binding Corporate Rules and the ICO's new UK approach. By **Laura Linkomies**.

The starting point for the Workshop was that the ICO issued a document on its new approach to Binding Corporate Rules (BCRs) on 25 July 2022[1], including simplifications for organisations. While the ICO regards BCRs as "the gold standard" and was a driving force to get this concept developed at European level for almost 20 years (*PL&B International* August/September 2004 p.13), it now

Continued on p.3

Ghost in the machine: Guidance on using AI recruitment systems

Edward Machin of Ropes & Gray assesses how the Information Commissioner's guidance on artificial intelligence and data protection applies to organisations' recruitment practices.

In 2012, the American software engineer and entrepreneur Marc Andreessen predicted that the rise of the Internet would put jobs in two categories: people who tell computers what to do, and people who are told what to do by computers. With that prediction continuing to prove correct, I wonder whether there is a similar prognostication to be made on the ubiquity of artificial intelligence (AI). The recent ChatGPT[1]

Continued on p.6

Issue 125 **JANUARY 2023**

UNITED KINGDOM
report

ISSUE NO 125 **JANUARY 2023**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Edward Machin
Ropes & Gray LLP

Gareth Oldale and Tillie Clark
TLT LLP

Claire Saunders and Jenai Nissim
HelloDPO

Richard Jeens, Ross O'Mahony and Alex Buchanan
Slaughter and May

Alexander Dittel
Wedlake Bell LLP

Dr Guido Reinke
A data culture advocate

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

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

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

ISSN 2047-1479

comment

Spotlight on Artificial Intelligence

It was noticeable at our planning meeting this month how many of the speaking proposals we had received for *Who's Watching Me*?, our 36th Annual Conference 3-5 July (p.22), had aspects of AI in them. The technology certainly impacts our lives already in so many ways. The ICO is now saying that AI technology is no longer a new issue, and compliance with data protection law is required on all aspects (p.11).

On p.1 our correspondent assesses the ICO's guidance on using AI recruitment systems. Bias is one of the essential questions to consider. We await the government's White Paper on AI - it will be interesting to see how it suggests tackling this issue. A recent paper from the Oxford Internet Institute comes to the conclusion that the current discrimination laws fail to protect people from AI-generated unfair outcomes. The author, Professor Sandra Wachter, highlights that AI is creating new digital groups in society – algorithmic groups – whose members are at risk of being discriminated against.[1]

How skillful is AI-based ChatGPT? The law firm Linklaters took a closer look to see whether the technology can also tackle legal questions[2]. There was a broad range of results from the surprisingly good to the bad, they say. To the lawyers' relief, it cannot, at least for now, advise their clients to the level of detail they need.

Also looking into the future is the article on the DPO role and function on p.13. Those in the role already know that DPOs are increasingly required to have not just legal knowledge but also expertise in other areas.

Privacy Laws & Business held a very successful Workshop in December together with law firm Hogan Lovells on Binding Corporate Rules (p.1). The Workshop identified differences between the UK and the EU regimes, and made recommendations for achieving the ideal of harmonisation or mutual recognition. We have now sent a memo to the European Data Protection Board, the ICO, Ireland's Data Protection Commission and the UK government.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

1 *www.oii.ox.ac.uk/news-events/news/ai-creates-unintuitive-and-unconventional-groups-to-make-life-changing-decisions-yet-current-laws-do-not-protect-group-members-from-ai-generated-unfair-outcomes-says-new-paper*
2 *www.linklaters.com/en/insights/blogs/digilinks/2022/december/chatgpt—-50-questions-to-road-test-its-legal-advice*

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 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

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

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

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

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

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

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

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

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

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

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

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

privacylaws.com/reports

"I've always found *PL&B* to be a great resource for updates on privacy law issues, particularly those with a pan-EU focus. It strikes the right balance for those in-house and in private practice. The content is clear, well presented and topical."

Matthew Holman, Principal, EMW Law LLP

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 36th year. Comprehensive global news, currently on 165+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

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

Subscriptions

Subscription licences are available:

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

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

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