Artificial Intelligence: A push for regulation

Josephine Jay and Christopher Foo of Wilson Sonsini Goodrich & Rosati analyse the developments that are likely to culminate in a series of legislation and guidance at EU and national level.

Until recently, artificial intelligence (AI) had not in itself been the subject of EU or Member State guidance, let alone legislation. Instead, it is covered by broader laws, including those addressing product liability, consumer protection and privacy. The GDPR, for example, was deliberately drafted to be “technology neutral” to ensure it covered emerging technologies like AI, without tackling them head on. This is perhaps unsurprising, given AI’s relatively recent pre-eminence. This is further combined with the difficulties that arise in defining AI, let alone explaining how it works and how it should be regulated.

This is set to change in the coming years, with EU bodies and regulators and the UK’s ICO accelerating their efforts to bridge this gap. At the EU level, this drive began in 2017 partly as a result of competitive pressures from the United States and Asia, and was spurred on by the appointment of Ursula von der Leyen to the presidency of the European Commission in late 2019. The UK similarly seems to have recognized that the existing legislative measures, creating data pools, and increasing greater transparency, expanding definitions of safety to cover AI-generated risks, and allocating responsibility for AI-based products and services. The Commission identified high risk sectors and applications for closer scrutiny as part of a risk-based approach to regulating AI.

The Parliament’s call was echoed by the European Council, stressing “a sense of urgency” for the Commission to put forward a European approach to AI by early 2018. In April 2018, the Commission began on a “Coordinated Plan” to guide the growth and implementation of AI in Europe. In June, the Commission established a High-Level Expert Group, comprising of representatives from academia, civil society and industry, to support this initiative, which released both the Ethical Guidelines for Trustworthy AI, Policy and the Investment Recommendations for Trustworthy AI in the first half of 2019. The Commission also presented a plan to boost “made-in-Europe” artificial intelligence.

Early 2020 saw a flurry of activity, in part aided by Ursula von der Leyen’s intention to propose AI legislation within the first 100 days of her taking office. This culminated in February 2020 in both the White Paper for Artificial Intelligence (White Paper) and the European Strategy for Data (Strategy), with the Strategy setting out a date for a proposed Data Act in 2021.

Key privacy recommendations: In its White Paper and Strategy, the Commission recognizes that a balance is needed between the needs of legislating for AI, increasing data sharing between and across the public and private sectors, creating data pools, and increasing investment. The White Paper and Strategy make a number of suggestions that will impact privacy, including:

- Expanding the GDPR data portability right. As AI use increases, so does the amount of generated personal data, and expanding data portability rights can give individuals additional control over the access and use of machine generated data. Such an amendment may be contained in the proposed 2021 Data Act.
- Increased data sharing. The Strategy calls for increased (privacy compliant) data sharing via changes introduced in the proposed 2021 Data Act, both within and between sectors. This could even be made compulsory in certain circumstances, e.g. when competition law fails to address the issue. Such compulsory data sharing should only occur under “fair, transparent, reasonable, proportionate and/or non-discriminatory conditions”, with the legitimate interests of the data holder to be taken into account.
- Facial recognition. The Whitepaper suggests permitting the use of facial recognition “where such use is duly justified, proportionate and subject to adequate safeguards”. The Commission intends to explore the topic further in a future Europe-wide debate.

United Kingdom

The UK first examined the interplay between data protection and AI in a 2017 report on the data protection implications of big data, AI and machine learning. Listed as a priority in its Technology Strategy 2018-2021, the ICO recognizes that organizations require greater accountability in their use of AI to keep pace with the GDPR’s strengthened data subject rights. As such, it considers the explainability of AI decisions to be a key area of its Framework. In 2018 the ICO began work on Project explAIIn to help organizations explain
their use of AI, and in early 2019 started to develop the Framework.\textsuperscript{18} The ICO consistently sought industry feedback through participation and consultations, while publishing a series of blog posts on the topic.\textsuperscript{19}

**The UK Auditing Framework:**
The challenges of allocating responsibility for AI and increasing transparency behind AI are interrelated as certain AI (such as AI with opaque or inaccessible inner workings, also known as “black box” AI) make it difficult to ascertain where liability for AI errors should lie and how to explain the decisions taken by algorithms. The EU Council and Commission have proposed that Member States should develop auditing techniques to identify unlawful outcomes produced by AI.\textsuperscript{20}

In March 2019, the ICO set about developing an auditing methodology for AI applications. The publication of blog posts that identified data protection challenges specific to AI, along with industry engagement, led to the publication of the Framework at the start of 2020, on the same day as the EU’s Strategy and White Paper.\textsuperscript{21}

The Framework provides pragmatic guidance to organizations participating in the AI sector, recognizing that although not every risk may be eliminated, trade-offs must be justifiable and recorded, and that each use case brings about different data protection implications and consideration.\textsuperscript{22} Organizations should review the Framework, including in relation to handling common pitfalls. Key privacy takeaways are:

- DPIAs are generally required. The use of AI to process personal data is likely to result in a high risk to individuals’ rights and freedoms, and thus requires a DPIA prior to processing personal data.\textsuperscript{23} DPIAs are a useful tool to identify the risks, to evaluate whether risks can be sufficiently mitigated, and to document an organization’s compliance with the law.\textsuperscript{24} If such risks cannot be sufficiently mitigated, the ICO warns organizations that they may have to halt their AI project and consult with the ICO before they can proceed.\textsuperscript{25}
- Establishing controllership. Companies often use AI run by third parties as opposed to AI that has been developed in-house.\textsuperscript{26} This may lead to some confusion on identifying the controller. The Framework provides that the nature of the AI service will be indicative. For example, organizations that provide AI development tools are likely to be processors, whereas organizations providing AI prediction services are likely to be controllers. The latter is particularly true when customers do not have sufficient influence over the “essential elements and purposes of the processing involved in the prediction”, or when such processing is only necessary to create and improve AI models (whether done at the outset or after the provision of a service).\textsuperscript{27}
- Appropriate lawful basis. Different lawful bases of processing may apply to the training of AI and the deployment of AI. For example, consent may be obtained for an organization to train facial recognition AI, but if that AI is deployed for multiple purposes (such as the monitoring of crime or to tag friends on a social network) each application may require a separate lawful basis.\textsuperscript{28} The Framework further notes that the performance of a contract may not be an appropriate lawful basis to train an AI if the service offered may perform sufficiently well without being trained on personal data: legitimate interests would be more appropriate.\textsuperscript{29} The Framework also recommends organizations to assess whether their use of AI constitutes solely automated decision making that would have a significant impact on individuals. If so, such processing may only be carried out on the basis of explicit consent, necessity for the performance of a contract or if it is authorized by applicable law, as long as individuals are adequately safeguarded.\textsuperscript{30}
- Data minimization compliance. The use of AI typically involves processing large amounts of data which presents inherent risks.\textsuperscript{31} The Framework recommends that organizations should narrowly identify the purpose of processing undertaken by the AI, and only process data necessary for that purpose. In the context of training AI, organizations should train AI only on the most relevant features of a data set. The fact that certain data may serendipitously prove to be useful cannot justify the use of it at the outset, unless an organization has identified a justifiable foreseeable event that such data would be relevant for.\textsuperscript{32}
- Ensuring individual rights. AI poses a challenge to data rights. AI may strip identifying information from data sets, whilst remaining personal data, and thus harder to link to and provide to an individual.\textsuperscript{33} Although organizations should not write off requests relating to such data as manifestly unfounded or excessive merely on the basis of their additional difficulty, some limitations are necessary.\textsuperscript{34} Where an AI model is designed to contain personal data, easy retrieval of an individual’s personal data should be inbuilt.\textsuperscript{35} Where personal data has been used to train AI however, requests to exercise individual rights to access may not be fulfilled if an individual cannot be identified without additional information.\textsuperscript{36} Similarly, if the data provided by an individual has been sufficiently transformed into code, data portability may not apply.\textsuperscript{37}

**AI Explainability Guidance:** The Guidance consists of three sets of guidelines that set out the basics behind AI explainability. It considers the ability to make such explanations vital to comply with the law, build trust and awareness among individuals and wider society, and as a part of good internal governance.\textsuperscript{38}

Key takeaways from the Guidance are:

- The extent and type of explanations required depend on the AI’s use case. Building on earlier stakeholder consultations, the Guidance, like the Framework, recognizes that context will be key in determining the substance of any explanations. For instance, using AI in recruitment would require explanations regarding rationale and responsibility, with bias being a sector-specific concern, whereas using AI in a medical diagnosis may require the
same explanations but with differing concerns over safety and performance, and the timing of such explanation.39

- Black box AI requires additional consideration. The ICO specifically warns against the use of “black box” AI unless an organization has thoroughly considered the risks and have prepared themselves sufficiently for the responsible design and implementation of such models.40 Supplemental tools for interpretation should be incorporated and used to understand the interaction between the model’s component parts.
- Organizations should document the measures they implement to explain AI. Organizations should ensure appropriate policies are in place to appropriately explain AI in accordance with the Guidance, for example by allocating responsibility to certain staff members, and offering training.41 The Guidance also recommends documenting each stage of the decision-making process in order to demonstrate accountability.42

**What next?**

Both the EU and UK are still in the process of gathering feedback on their latest AI publications. The activity of the European legislative bodies since 2017 indicates that a series of legislation and guidance will be forthcoming. The White Paper and Strategy are open to public consultation until 31 May 2020, after which the Commission will propose a revised version of the Coordinated Plan by the end of 2020.43 The first iterations of the anticipated Data Act, likely to govern data access and sharing, are expected next year, as part of a broader suite of legislation tackling AI.

In the UK, the ICO’s Framework and Guidance are still in draft form. The finalized versions are anticipated later this year, although they are not expected to have major divergences from the currently published versions.

**REFERENCES**

6. Note 1, page 17-18
13. Note 11 page 12-23 and Note 2 page 7
15. Ibid, page 13

**AUTHORS**

Josephine Jay and Christopher Foo are Associates at Wilson Sonsini Goodrich & Rosati.
Email: jjay@wsgr.com, cfoo@wsgr.com
Calls for primary legislation for Coronavirus app

A rapid evidence review published by the Ada Lovelace Institute sets out proposals for whether, and how, the UK government should use technology to transition from the Covid-19 global public health crisis. Whilst the government and NHSX are planning to introduce a contact tracing app, the Institute stresses the need for primary legislation to address the societal implications properly.

The Institute says that “there is no evidence to support the immediate deployment of digital contact tracing or immunity certification and calls for the establishment of a new Group of Advisors on Technology in Emergencies (GATE) to oversee the development and testing of any proposed digital tracing application.”

Carly Kind, Director of the Ada Lovelace Institute said: “The government is right to explore non-clinical measures in its response to the Covid-19 crisis, but it must take action to ensure technological applications, such as the proposed NHS rollout of digital contact tracing, do not become counter-productive because of a failure to take account of both the barriers to deployment and the full impact on people and society.”

The review recommends that the deployment of Covid-19 technologies should be subject to the sign-off of the Group of Advisors on Technology in Emergencies (GATE) which would consider the effectiveness of any tool within the context of diagnostic testing capacity and after an assessment of its likely adoption. GATE would also make recommendations about how to ensure technologies protect privacy by design and by default.

A draft Coronavirus (Safeguards) Bill has been prepared by Professor Lilian Edwards, University of Newcastle, and other academics, but it is not yet (end of April) on the Parliamentary agenda.

Let's see the draft Bill at osf.io/preprints/doi:arxiv/ye66v/

Alan Turing Institute to research digital identities

The Alan Turing Institute announced on 29 April that it will take part in a research programme which seeks to enhance the safety and security of digital ID systems by drawing on the UK’s expertise in privacy enhancing-technologies, and data-driven cybersecurity. The project will focus on three key outcomes:

• Research to generate new knowledge aimed at enhancing the safety and security of digital ID systems, including exploratory areas such as encryption technologies and real-time threat modelling.

• Development of an open source library of technical tools in collaboration with existing open source digital ID providers.

• Piloting of new privacy and security features in partnership with technical providers and select countries. This project is funded through a £4.3 million grant from the Bill & Melinda Gates Foundation.

See: www.turing.ac.uk/research/research-projects/trusted-digital-infrastructure-identity-systems
Returning to work: Covid-19 and the UK data protection perspective

Nicola Fulford and Hannah Jackson of Hogan Lovells report on the data protection aspects organisations should consider with regard to coronavirus testing and processing of health data.

Individually, many of us use data to track our progress – from fitness gains to home energy consumption; we watch information about our lives and use it to inform our activities. On a larger scale, numerous organisations have made significant investments in data analytics capabilities, and at a state level, a vast quantity of information about populations is used to direct public policy. It is not unreasonable,

Continued on p.3

Winner of the ICO’s Data Practitioner Award: Barry Moult

The regulator’s annual award recognises a long career in NHS Information Governance and innovative thinking. Laura Linkomies talked to Barry Moult about his work.

The 2020 ICO Practitioner Award for Excellence in Data Protection was awarded to Barry Moult, Information Governance and Privacy Consultant, and former Head of Information Governance and Health Records at the Colchester Hospital University NHS Foundation Trust. Recently retired from his role at Colchester, which he held from 2014 to 2018, Barry is now utilising his decades-

Continued on p.5

PL&B Recruitment Service

PL&B has many privacy professionals seeking new opportunities. Our recruitment service ranges from advertising your vacancy to the complete recruitment lifecycle.

• Advising on job specifications, defining your ideal candidate
• and skill set, salary banding and benefits
• Identifying, screening and shortlisting candidates
• Liaising between you and the candidates, arranging interviews and communicating feedback.

privacylaws.com/recruitment

PL&B Services: Conferences • Roundtables • Content Writing
Recruitment • Consulting • Training • Compliance Audits • Research • Reports
Stay alert to Covid-19 data protection issues

There is unfortunately still much uncertainty about when we are back to "normal" life in the UK. The 'new normal' will most definitely include new rules and procedures at the workplace when offices start to reopen. Read on p.1 our correspondent's analysis of the data protection implications at the workplace.

We recently carried out a survey to find out about the challenges that DPOs encounter due to the pandemic. There are implications across the board: for remote working, data security, processing employee data etc. Read on p.12 how organisations are tackling these issues.

Normal compliance work, for example processing Subject Access Requests has not gone away – in fact some organisations are seeing an influx of requests relating to furloughing and employee health records (p.9). While employers may ask staff whether they have Coronavirus symptoms, they should not ask unrelated questions, for example about underlying medical conditions, or symptoms not associated with Covid-19. The NHSX contact tracing app may help to control the virus but has privacy implications (p.8).

If home working and social distancing continues for the rest of the year for many, it will undoubtedly create a new work culture in some organisations. DPOs may become more reliant on webinars and online team meetings to exchange information. Privacy Laws & Business will soon launch a value-added way for you to connect with our expert consultants to address your specific questions during an initial half-an-hour consultation.

In this issue, to keep you well-informed, we bring you updates on AI legislative developments (p.16), how to choose your legal basis for adtech (p.22), the implications of the Supreme Court’s Morrisons vicarious liability decision (p.24), top tips on managing data breaches (p.27), data protection issues for SMEs (p.20), DP issues in scientific research (p.29) and an interview with the ICO award winner (p.1).

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


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

Stay informed of data protection legislative developments.
Learn from others’ experience through case studies and analysis.
Incorporate compliance solutions into your business strategy.
Learn about future government/ICO plans.
Understand laws, regulations, court and tribunal decisions and what they will mean to you.
Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually
2. Online search by keyword
   Search for the most relevant content from all PL&B publications and events. You can then click straight through from the search results into the PDF documents.
3. Electronic Version
   We will email you the PDF edition which you can also access via the PL&B website.
4. Paper version also available
   Postal charges apply outside the UK.
5. News Updates
   Additional email updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.
6. Back Issues
   Access all PL&B UK Report back issues.
7. Events Documentation
   Access UK events documentation such as PL&B Annual International Conferences, in July, Cambridge.
8. Helpline Enquiry Service
   Contact the PL&B team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

PL&B UK Report offers excellent guidance for Information Management professionals on the latest changes in data regulation, as well as useful advice on improving data security and protecting privacy.

Simon Baker, Nursing and Midwifery Council

International Report

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

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

Subscriptions

Subscription licences are available:
• Single use
• Multiple use
• Enterprise basis
• Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe.

Satisfaction Guarantee

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