ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS

DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Issue 132 MARCH 2024

Spotlight on cookies: An increased regulatory focus

As the ICO warns organisations that use advertising cookies, **Emma Erskine-Fox** of TLT advises on how to ensure cookie compliance and avoid regulatory action.

The rules on cookies may not have substantively changed since 2011, but regulatory guidance has significantly evolved in the last few years, addressing concerns with increasingly intrusive uses of these technologies to track individuals and send them ads.

Recent developments have brought this issue, previously seen as a low-risk area, to the forefront of many organisations' and privacy

Continued on p.3

AI and ADM: No transparency and no choice?

Alexander Dittel of Wedlake Bell LLP discusses how privacy notices should address the processing of personal data relating to machine learning, artificial intelligence and automated decision-making.

As transparency and choice are two of the essential principles of data protection law, their implementation in relation to AI and ADM raises several issues. These challenges are similar to those encountered in training machine learning (ML) models over the last ten years.

The large-scale collection of public data for the training of ML/AI models is at the core of this discussion. The

Continued on p.5

UNITED KINGDOM **report**

ISSUE NO 132 **MARCH 2024**

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
Emma Erskine-Fox
TLT LLP
Alex Dittel
Wedlake Bell LLP
Sally Annereau
Taylor Wessing LLP
Paul McGrath, Pilar Arzuaga and Charlotte Moorhouse
McDermott Will & Emery LLP
Rebecca Cousin, Lucie van Gils and Ian Ranson
Slaughter and May
Katie Hewson, Daniel Jones and Nelson Kiu
Stephenson Harwood LLP
Richard Field
Appleby

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

UK to legislate on advanced AI 'when the time is right'

The UK aims to be a Science and Technology Superpower by the end of the decade. The government continues to believe that a light-touch regime is the best way to achieve this aim – in stark contrast to the EU's world-leading new AI Act. Issuing its response to the AI White Paper consultation on 6 February, the government also announced a £100 million package to help realise new AI innovations and support regulators' work on AI. The government says this will help them to develop cutting-edge research and practical tools to address AI risks.

The government says it will not want to rush into legislating before it fully understands the risks and opportunities of AI. "However, the challenges posed by AI technologies will ultimately require legislative action in every country once understanding of risk has matured." Therefore, legislation may in time be introduced for highly capable GenAI.

For now, the government continues on its pro-innovation path asking existing regulators to apply cross-sectoral principles. Regulators will need to outline their strategic approach to AI by 30 April 2024.

In the meantime, organisations need to tackle practical problems such as revising privacy notices in light of using AI and automated decision-making p.1). AI is also a game-changer in staff selection and recruitment (p.12).
Amongst all the challenges, we can celebrate the renewed adequacy decisions for Guernsey (p.21), Jersey and Isle of Man, and the modest reliefs to companies' subject access compliance burden, as proposed in the Data Protection and Digital Information Bill (p.10).

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.

AI and ADM... from p.1

legal justification for such processing is undergoing renewed scrutiny, particularly following the launch of OpenAI's ChatGPT in November 2022. On the other hand, ADM raises questions regarding the level of transparency about its logic and effects on individuals.

Many organisations could be forgiven for adopting a "wait-and-see" approach with the UK government's constant pro-innovation rhetoric. The research exemption under the UK GDPR already allows repurposing data for ML/AI model training. It exempts the controller from transparency to the extent that compliance would be impossible or seriously impair the research.[1] However, the UK data reform proposes to further expand the exemption and dilute the concept of "personal data"; thereby practically removing any transparency or choice requirement. However, existing rules and emerging good practice cannot be ignored by larger organisations, particularly with the growing body of international guidance and the leadership in AI regulation by China[2] and the European Union.

Whilst UK courts and regulators are not bound by any European Union data protection case law or regulatory decisions made after 31 December 2020, they continue to be persuasive.

Transparency under the UK GDPR

Transparency rules consist of three distinct but interdependent principles of fairness, lawfulness and transparency. Transparency disclosures must be drafted in "recognising the reasonable expectations of the data subjects, considering possible adverse consequences processing may have on them …"[3] and ensuring the processing is not "unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject".[4]

However, commercial organisations will pay particular attention to the exemptions and workarounds. For example, the "impossibility" exemption[5] could apply if informing individuals about collecting their data from the public domain for the training of ML/AI models, becomes impossible or involves disproportionate effort. Yet despite this exemption, the Information Commissioner's Office (ICO) notes that if the controller carries on a business model which depends upon mass collection of data, it cannot assert that compliance would be disproportionately burdensome.[6]

Further, many controllers may avoid transparency by adopting the view that their training data is "de-identified" or "anonymised". The UK data reform will further strengthen this position by enabling organisations to determine that at the time of processing, identification of an individual is not possible and no personal data is processed.[7] Synthetic data will not constitute personal data, as recently confirmed by the Court of Justice of the European Union (CJEU) in the *NVSC* case.[8] Shifting transparency and choice obligations on the third party AI provider by referencing such party in the privacy notice could also work. However, the controller could still face liability if it acts as a joint controller who "participated in the determination of the purposes and means" of the processing.[9]

If the training takes place outside the UK it will not be caught by UK GDPR unless it relates to the offering of goods or services or the monitoring of behaviour of individuals in the UK. Certain automated mathematical processes such as automated indexing will likely not relate to such activities and will not be subject to the UK GDPR.[10] Finally, the UK GDPR also recognises that a previously undeclared "compatible purpose" may be lawful in the context of the training of ML/AI models. Whilst this may apply to historic data, a general notice about the processing should be available to the public.

"… to improve and develop our products …"

The wording "… to help us provide, support and improve … our services" is often seen in privacy notices to describe the use of data for service development. Being rather obscure, it does not capture the complexities of training data, input data, benchmark data and output data in the ML/AI lifecycle. According to the Information Commissioner's office (ICO), such wording is "unlikely to be considered transparent" if people are not told that their data is used to train and test ML/AI systems.[11] A privacy notice should address the following ML/AI themes:

- **Development of AI and ML models**, for example, by referring to "… analysis, machine learning, product development, artificial intelligence research, and testing", or "… personalised recommendation algorithm".
- The **use of training data from the public domain**, for example, by referring to ML/AI training data from "publicly available sources", which is a mandatory disclosure under the UK GDPR, and public data will constitute personal data.
- **Ingesting user content for ML/AI training**, for example, by explaining the "use [of] Content you provide us to improve our Services, for example to train the models ….". Presenting a table of purposes and corresponding data in the notice could obscure to the untrained eye the fact that "User Data" is used to " … develop and improve our personalised recommendation algorithms …". Any confusing language will not escape public scrutiny, as experienced by the video conferencing platform Zoom last year when it changed its terms to imply user consent to using "customer content" for "product and service development, marketing, … machine learning, artificial intelligence, training, …". Adding that "Notwithstanding the above, … will not use audio, video or chat Customer Content to train our artificial intelligence models without your consent" did not help, because it was unclear if implied or express consent was relied on. The platform's subsequent clarification posted in a blog probably failed to convince the sceptics.
- **Describing what happens with data in training and how it might affect the individual** helps to put any privacy risk into perspective. OpenAI explains that "… it learns about associations between words, and those learnings help the model update its … weights [which help it] to predict and generate new words in response to a user request. … much like a person who has read a book and sets it down, our models do not have access to training information after they have learned from it."[12]
- **Privacy safeguards** will help minimise personal data. OpenAI explains that "…models may learn [from names of famous people]…to understand how things like names and addresses fit within language and sentences…". However, steps are taken to "… reduce the processing … when training … remove websites that aggregate large volumes of personal information and … train our models to reject requests for private or sensitive information about people."[13]
- Each ML/AI activity could attract a different **lawful basis**. Recently, in *Digi*,[14] the CJEU suggested that creating a copy of the customer database to conduct A/B tests and correcting errors in subscription files, was related to the performance of the subscription contract because these errors could have consequences for the performance of the contract. Whilst this could arguably apply to some ML/AI activities, *WhatsApp* previously failed to establish that its service improvement was necessary to perform the contract, which would set a "dangerous precedent" in depriving individuals of the right to opt-out.[15] Whilst legitimate interest comes with the right to opt-out, if the training data includes user content or sensitive private information, the consent requirement under the UK GDPR could be triggered. The ICO highlights the ethical need for consent in research even if consent is not the lawful basis.[16] AI leaders such as OpenAI offer a way to object to having one's public data used for training.[17] Recently, the Italian *Garante* reopened its investigation of OpenAI and it may consider if opt-out is appropriate given the invisible nature of the processing and the lack of awareness among the public.[18]

"… TO RECOMMEND SERVICES THAT MIGHT BE OF INTEREST TO YOU …"

ADM such as recommender engines typically only have a trivial effect on the individual. However, an analysis or prediction of personal aspects, including income bracket, propensity to offending, safety of driving, likelihood of fraud etc., could give rise to significant effects on the individual, especially if the machine gets it wrong.

Credit scoring clearly has such significant effects. However, in a recent court case in Germany, SCHUFA tried to argue that since the decision about offering credit is actually made by the bank, the credit referencing agency was not engaging in ADM. The CJEU disagreed and held that the "… automated establishment … of a probability value based on … ability to meet payment commitments … where a third party … draws strongly on that … " information does constitute ADM.[19]

Under the UK GDPR, ADM attracts additional transparency requirements, but only if it is "based solely on automated processing …" and "produces legal effects … or similarly significantly affects …". Controllers often argue there is no significant effect or that there is a human in the loop. However, a "symbolic" human in the loop will not disengage the ADM rules in Article 22.[20] Once triggered, the ADM provisions require "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" and implementing safeguards to protect the individual's legitimate interests, obtaining human intervention, to express view and contest the decision. Arguably, regardless of Article 22 being triggered, transparency under the UK GDPR requires similar information to be disclosed.

An appropriate privacy notice for ADM

Generally, a privacy notice should address the following ADM themes:

1. Understanding **what input data is relied on to generate the output** can help the data subject challenge the accuracy of the output. In practice, however, controllers will only offer categories of data such as

“credit performance data”, “the transactions made on the current accounts” or “fraud prevention indicators”.

2. Often the inferences generated about the individual remain undisclosed, contrary to the ICO’s push to explain “design fairness” in the algorithmic architecture.[21] Such information about **how the model is trained** could reveal a risk of bias, discrimination or unfairness. OpenAI explains “… we might have a model try to complete … sentence … learns from many lines of text, … it can predict the next word more accurately. It then repeats this process across a very large number of sentences. …”.
3. **Why a decision is made and on what logic** is often considered a trade secret. The Amsterdam Court of Appeal recently held that information about explanation of algorithmic decisions cannot be withheld as a trade secret, because it would be disproportionate to the negative effects of unexplained automated dismissals of workers. In this case, the drivers’ ride hailing app accounts were blocked based on opaque algorithmic fraud scoring.[22] Of course, the black-box nature of a neural network and reliance on its hidden layers means the weighing of data points is unknown. Here, SCHUFA explains the general purpose of its scoring which involves the “… forecasting [of] future events and behaviour on the basis of information that has been collected and past experience” and “to help determine the likelihood that a consumer with certain characteristics will act in a way that will produce certain outcomes”.
4. **Explaining the consequences** of ADM, such as “… deactivation of users (generally only after human review)” is critical for any fair notice.
5. It will be important to explain which **safety and performance measures** are in place to ensure correctness of ADM. Microsoft explains that “… we manually review some of the predictions and inferences produced by the automated methods against the underlying data from which the predictions and inferences were made. …”. SCHUFA says “…the methods used are mathematically and statistically recognised and scientifically sound. Independent external experts have confirmed the scientific validity … procedures … are disclosed to the competent supervisory authority. … regularly checking the quality and currency of procedures in use, and making appropriate updates, …”.
6. Providing an easy way to **object to or challenge decisions** must be ensured for qualifying ADM. Implementing an effective alternative, be it opt-out or human review, presents a real challenge in ADM.

The lawful basis for “low-risk” ADM might be legitimate interest. However, for qualifying ADM it is limited to consent, contract or legal obligation. In the earlier *SCHUFA* decision, the CJEU doubted if German law provides for a sufficient legal obligation, but left it to the referring court to decide upon. In contrast, in its recent Content Moderation Guidance, the ICO presented a narrower interpretation of qualifying ADM which may not include a tool operating “according to specific, pre-defined parameters representing things that humans have already decided on”.[23]

Conclusion

Data protection transparency is guided by the need to provide as much information as possible, while doing so in the most concise way possible. In practice, it is viewed as a flexible concept influenced by regulatory action on the one hand and commercial realities, such as risk of claims, on the other.

Available workarounds and an ever-relaxing regulatory environment in the UK probably contribute to the silence in privacy notices about the complexities of ML/AI and ADM. Unfortunately, major UK organisations engaging in ML/AI activities and ADM fail to make appropriate disclosures in their privacy notices. As a result, data subjects end up with no transparency and certainly no choice.

Nevertheless, the overarching concept of fairness requires clear language instead of complex privacy notices which are hard to navigate. A separate comprehensive section about ML/AI in the privacy notice might be more transparent than piecing together various disclosures from across the privacy notice. As a result, data subjects will at least have some transparency and perhaps some choice.

AUTHOR

Alexander Dittel is a Partner in Technology at Wedlake Bell LLP.
Email: adittel@wedlakebell.com

REFERENCES

[1] ICO’s Detailed guidance on the research exemption, May 2023 ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/the-research-provisions/

[2] Chinese Regulation on recommendation algorithms (2021), Rules for deep synthesis (synthetically generated content) (2022), and The Interim Measures for the Management of Generative Artificial Intelligence Services (2023).

[3] EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, 8 October 2019 edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[4] EDPB Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, version 2, adopted on 20 October 2022.

[5] Article 14(5)(b) of UK GDPR.

[6] ICO’s Enforcement notice against Experian, October 2020 ico.org.uk/media/action-weve-taken/enforcement-notices/2618467/experian-limited-enforcement-report.pdf and *PL&B UK Report*, March 2023, p.1.

[7] Data Protection and Digital Information Bill bills.parliament.uk/bills/3430

[8] Case C-683/21 *Nacionalinis visuomenės sveikatos centras prie*

REFERENCES

Sveikatos apsaugos ministerijos v Valstybinė duomenų apsaugos inspekcija curia.europa.eu/juris/document/document.jsf?text=&docid=280324&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7438261

9 As above.

10 *Clearview AI Inc v The Information Commissioner* [2023] UKFTT 00819 (GRC) caselaw.nationalarchives.gov.uk/ukftt/grc/2023/819

11 ICO's Explaining decisions made with AI ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/

12 How ChatGPT and Our Language Models Are Developed, OpenAI help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed

13 As above.

14 C-77/21 *Digi Távközlési és Szolgáltató Kft. V Nemzeti Adatvédelmi és Információszabadság Hatóság* curia.europa.eu/juris/document/document.jsf?text=&docid=267405&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1913383

15 In the matter of JG, a complainant, concerning a complaint directed against WhatsApp Ireland Limited in respect of the WhatsApp Service, DPC Inquiry Reference: IN-18-5-6 (12 January 2023) www.dataprotection.ie/sites/default/files/uploads/2023-04/WhatsApp%20FINAL%20DECISION%20%28adoption%20version%29%20Redacted.pdf

16 Note 1.

17 OpenAI Personal Data Removal Request share.hsforms.com/1UPy6xqxZSEqTrGDh4ywo_g4sk30

18 ChatGPT is violating Europe's privacy laws, Italian DPA tells OpenAI, 29 January 2024 techcrunch.com/2024/01/29/chatgpt-italy-gdpr-notification/ and *PL&B International Report*, June 2023, p.1.

19 Case C-634/21, SCHUFA Holding AG, CJEU curia.europa.eu/juris/document/document_print.jsf?mode=lst&pageIndex=0&docid=280426&part=1&doclang=EN&text=&dir=&occ=first&cid=907530.

20 Case 200.295.742/01, *Uber B.V. v appellants*, Amsterdam Court of Appeal, 04-04-2023 uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2023:793 (in Dutch)

21 Note 11

22 Case 200.295.742/01, Uber B.V. v appellants, Amsterdam Court of Appeal, 04-04-2023 uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2023:793

23 Content moderation and data protection, ICO, 7 February 2024 ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/online-safety-and-data-protection/content-moderation-and-data-protection/

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.

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.

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.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked at least 10 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

> Given the rate of change in law, regulation and business practice, it is essential to have concise and up to date information. *PL&B* is always relevant and continues to offer great value..
>
> **Adam Green, Chief Risk Officer, Equiniti**

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 37th year. Comprehensive global news, currently on 180+ 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.