AI deployment and transparency: A practical perspective

Claire Saunders and **Alison Deighton** of HelloDPO Law provide insights from their practice.

In its reflections on the generative AI consultation series it undertook last year, the ICO has (understandably) put a heavy focus on transparency in respect of AI.

In practice, it can be difficult to explain AI (generative or otherwise) in a meaningful way when the technology being deployed is complex, interactions with users or customers are brief and information is often having to be displayed on a mobile phone screen. So how do you ensure you provide individuals with the information they need when deploying AI in such a technically complex area? In the sections below we explore some of the practical steps that we have found useful when supporting our clients grappling with explaining AI tools.

Understanding the model

Before you can hope to explain the AI you are deploying, you must first ensure you have a proper understanding of how the model has been trained and how it operates in practice. For example, is the AI model a rules-based model that follows if-then rules to make decisions? Is the AI tool using machine learning to learn patterns from datasets and make predictions or decisions? Does the AI tool incorporate neural networks, which consists of multiple nodes which interconnect to process information and make decisions? Does the AI tool involve reinforcement learning, where the tool learns from its environment and feedback to improve its decision-making?

Once you understand how the model works (at a basic level at least!), you then need to ensure you have a good understanding of how personal data has been used to train the model and how personal data will be used in practice when the AI tool is deployed.

It is useful to have a list of AI due diligence questions to assist with obtaining the necessary understanding. The questions can be used with internal teams or with external suppliers who are providing AI tools. AI due diligence questions can also be used to test the way in which AI models have been trained to ensure the risk of bias is mitigated, and to ensure that training datasets have been procured and used appropriately. The questions should cover topics such as:

- Request for a model card to provide an overview of how the model works, the training data used, intended use of the tool etc. If the AI tool is being developed in-house, ask your engineers to produce model cards for the AI models they are developing.
- Information about training data used, including steps taken to ensure datasets are sufficiently large, diverse and representative for your intended use.
- If third party AI tools are used, whether input data and prompts provided by you will be used by the provider to train the model or provide output to third parties.
- Confirmation of the roles of the parties involved. Is an AI tool provider acting as a processor, controller or joint controller?
- For how long is data retained by a third-party AI provider? If AI models are developed in-house, for how long does the data need to be retained internally?
- Where is data that is input into the AI tool stored / transferred to? Are there transfers to third parties?
- If a data subject exercises their rights under the GDPR, how can this be accommodated by the tool? For example, if an access request is made, how can identifiable information be extracted? Can data be deleted if an erasure request is received?

This is, of course, not an exhaustive list and questions will need to be tailored to the AI which is being proposed.

You should also add information and reporting obligations into your contracts with AI developers to ensure you get the information you need on an ongoing basis to enable you to maintain an appropriate level of transparency with data subjects.

If you have obtained a model from a developer and work is being done to tweak the model in-house to make it more effective for your intended purpose, you need to understand what effect this has on the data processing undertaken so that you can adapt your approach accordingly.

> If there are multiple parties involved, it is obviously important to be clear about their roles (controller/processor/joint controller).

Don't forget the basics

When using personal data in the context of AI, organisations need to comply with the GDPR rules on transparency. The ICO in its guidance on transparency in AI states that at a high-level, organisations need to cover:

- Purposes
- Retention
- Recipients

There may be multiple purposes for the data processing, training, testing and developing the model as well as use in the model itself and potentially generation of new personal data. These purposes need to be clearly and separately outlined. If there are multiple parties involved, it is obviously important to be clear about their roles (controller/processor/joint controller) to ensure the individuals are aware who are the controllers for their data (so

that they can engage with them) and that privacy information is provided at an appropriate point by an appropriate party. You need to ensure you provide enough information to ensure your processing is fair and this may include an explanation of how the model works to process the data and why you chose to use AI.

There will be an element of risk assessment in considering what information needs to be conveyed in relation to purpose. You should consider the impact of the outcomes on the data subjects and how that affects how much information they may want to receive about the functioning of the tool. Consultation at this stage may assist in determining the value data subjects place on a detailed explanation. You should also consider how well understood the outcome is, a simple chatbot to help you with returning a product will be understood much better than a model which makes a significant decision based on a number of factors and this will affect the amount of information and explanation which needs to be provided.

Retention periods may not be as clear as in personal data use cases that are better understood and there may be concerns that once personal data enters an AI system it will remain there indefinitely.

Details of the recipients of the data are also likely to be important to people because they may not necessarily expect personal data to be disclosed in the way it will be in the use and training/development of the tool.

Using the information gathered in the due diligence phase, you should have been able to build a picture of the processing which will allow you to address these points and other necessary information to comply with the transparency requirements.

Whilst English law is currently based on existing rules, organisations should be aware that if their use of AI falls within the territorial scope, they will need to comply with transparency requirements in the EU AI Act.

Translating tech into plain English

Individuals need to be provided with clear, concise and understandable information. Providing this information is likely to involve tech and privacy personnel working together to explain complex technical functionality in language that the data subjects will understand. It is likely this will necessitate judgments being made about whether certain types of information will increase or hamper their understanding of the use of AI and should involve the exploration of different mechanisms for presenting these explanations to see if they can help to increase understandability. There may be technical explanations that do not occur to a data privacy professional, but which could be effectively deployed to increase transparency. If compromises are made in terms of being transparent and providing information people will understand, you should document the reasons why you chose the course of action (rather than other available options) in a DPIA so that you can demonstrate why such decisions were made.

There will be a need for continuing engagement between these teams and it may be advantageous to set up a forum in which tech and privacy personnel can come together on a regular basis to ensure the privacy team is kept apprised of updates and has the information it needs to ensure transparency is maintained.

> It may be advantageous to set up a forum in which tech and privacy personnel can come together on a regular basis.

Who is your audience?

This is always a consideration when complying with transparency requirements, but the technically complex nature of AI throws it into sharp focus.

If you are dealing with an audience whose level of sophistication is not high, don't underestimate the need to give some background information before starting the explanation of the processing itself. This could involve a basic explanation of what AI is and how it works, perhaps with a cheat sheet on key terms.

Training

If you are using AI, almost, if not all staff will need to understand, to varying degrees, how it works and how it is used by your business.

If you have customer/client facing staff who are likely to receive queries in relation to the use of the AI, they will need to have an understanding of how it works, to be able to respond to basic queries and to understand when they need to refer individuals to the privacy team.

Decision making

You will need to consider whether the use of the model involves making automated decisions with a legal or similarly significant effect under Article 22 of the GDPR, as this will increase the transparency obligations you need to comply with. This includes providing meaningful information about the logic involved in the decision as well as the significance and the envisaged consequences of such processing for the data subject.

The areas where we are most frequently seeing AI tools being used with such effects are in recruitment decisions and in credit and insurance businesses. In relation to recruitment, AI tools can be used to filter out or shortlist candidates. In the finance and insurance sectors AI tools have been used for some time to automate decisions about whether to offer credit or insurance and to determine the level of credit to be offered or the premium payable for a policy. AI tools are also used by social media platforms to detect and automatically block users who breach the platform's terms of use. All of these decisions have either a legal effect, for example, ending a contract due to breach of contract, or a similarly significant effect. An example is determining whether you are eligible for a particular job or whether you will receive a mortgage offer.

When explaining how AI is used for such decisions, the most challenging task is to explain the logic involved in the decision-making. In some cases, businesses will not wish to reveal too

much about the logic as this is their proprietary knowhow. The logic can also be difficult to explain when multiple factors will be applied to the decision and there may be several automated steps in the decision-making process. It may also be the case that it is difficult to find anybody within the business who can easily explain the logic deployed, especially if the AI tools used by the business have been developed by a third party. In its guidance on automated decision making, the ICO makes it clear that you should avoid confusing people with over complex explanations of algorithms. In these situations, the initial work done in the due diligence phase and building relationships with your tech colleagues should help to overcome these issues. Using responses to the due diligence enquiries and high-level logic information from the AI model card may be a good starting point for a suitable explanation to individuals and contractual requirements with third party developers to provide logic information should help you to fill gaps in explanatory information if any are discovered. Depending on the circumstances, information such as that concerning the robustness and reliability of decisions, accuracy, security of the model/system, steps taken to avoid bias and negative impact on the individual may also help the individual to understand the operation of the model.

Individuals will also need to have appropriate information so that they can exercise their right to obtain human intervention, to express their point of view and to challenge the decision. The ICO recommends explaining how people can do this at the time you provide the decision as this is the point at which individuals can make use of the information. For example, if you are using AI to review CVs and select/reject candidates, when the candidate receives the rejection, they should also be sent reminder that the decision was made using AI and be advised how they can express their view or challenge the decision (giving contact details for this purpose). The review needs to be carried out by someone who is suitably qualified and authorised to change the decision if this is necessary. The review should cover the facts on which the decision was made and take into account any additional evidence provided by the candidate.

The ICO has produced non-statutory guidance in conjunction with the Alan Turing Institute[1] which will be essential reading for those using AI to undertake decisions of this type and can be used more widely to help with complying with transparency requirements more generally. Even where decisions do not fall within the scope of Article 22, care should be taken to explain the AI and human elements of the decision-making process.

TLDR (Too Long; Didn't Read…)

Perhaps as important as what information you provide, is how you present it.

As is the case for any transparency exercise, the balance between conveying the information which you are required to give and not ending up with a situation where no one engages with it is a fine one.

This is another situation in which you should consider your audience, for example, younger people may find information presented via video an easy to digest approach, whereas a technically sophisticated audience may appreciate detailed technical information in text format.

A layered approach to privacy information which helps guide the data subject through the layers of complexity, to obtain the level of information which is right for them can be useful, especially where data subjects may have varying levels of sophistication.

Using just-in-time reminders to convey key messages is another technique which can work well, as can using FAQs as a quick reference guide.

Test and review

The best way to see if you have successfully managed to explain your use of AI is to test this on members of your target audience. Getting individuals to review the information and answer questions about their understanding of it should reveal any areas of weakness in the explanation. You should consider using this on an ongoing basis or devising a way of obtaining feedback from users which can be used to evaluate the transparency information over time.

The more significant the decisions being made by AI tools, the more important consultation with data subjects will be to ensure they properly understand how AI is being deployed. Organisations are often wary of undertaking consultation. However, it can be a powerful tool to help organisations develop more meaningful explanations. Consultation on AI and privacy matters does not need to be carried out as a stand-alone exercise. If an organisation already carries out user testing or has a customer panel for other purposes, these fora can be used to ask AI and privacy related questions. It can also be useful to embed AI and privacy feedback questions within wider user-testing journeys, as this will more accurately test how users are receiving and understanding information that is provided during their interaction with a product or feature.

Remember to keep your transparency measures under regular review to ensure they are updated with changes such as increased functionality or use of new/different personal data.

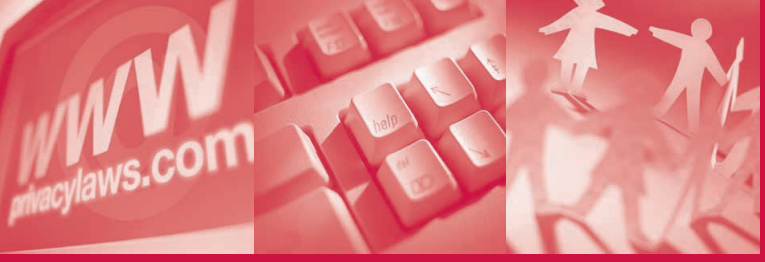
We are still in the very early stages of our AI journey, but adoption is rapid and deployers need to start paying more attention to how they approach transparency, putting strategies, policies and procedures in place to help them to deal with the inevitable proliferation in the uses and usage of this technology.

AUTHORS

Claire Saunders is a Professional Support Lawyer, and Alison Deighton is a Director and Co-Founder of HelloDPO Law.
Emails: clairesaunders@hellodpo.com
alisondeighton@hellodpo.com

REFERENCE

1 Guidance on AI explainability
www.turing.ac.uk/blog/project-explain-enters-its-next-phase
www.turing.ac.uk/news/project-explain/insights-from-phase-two



ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

ICO to develop codes of practice on Edtech and automated decision-making and AI

Government amends the Data Bill at the House of Lords by adding new provisions on children's data and direct marketing by charities. By **Laura Linkomies**.

The House of Lords made some amendments to the Data Use and Access Bill (DUAB), including to the definition of scientific research which is of great importance as the Bill would simplify the requirements for this type of data. The Lords made an

Continued on p.3

Why 2025 is the year to refresh your marketing compliance

Rebecca Cousin, **Bryony Bacon** and **Rosie Wilson** of Slaughter and May analyse the fast-evolving legal landscape for digital marketing and cookies.

The value of the UK advertising market is the largest in Europe[1] and is growing, with digital marketing spend in the UK projected to rise from £32 billion in 2024 to £44 billion in 2028 according to research by PWC[2]. Despite its clear commercial importance, for years digital marketing was an area of regulatory uncertainty. Long promised reforms to the e-marketing rules repeatedly stalled with the iterations

Continued on p.4

Issue 138 **MARCH 2025**

UNITED KINGDOM
report

ISSUE NO 138 **MARCH 2025**

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
Rebecca Cousin, Bryony Bacon and Rosie Wilson
Slaughter and May

Sol Pearson and Emma Erskine-Fox
TLT LLP

Victoria Hordern
Taylor Wessing LLP

Claire Saunders and Alison Deighton
HelloDPO Law

Fred Snowball, Tabitha Al-Mahdawie, Chris Akka, and Josie Duggan
Macfarlanes LLP

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

Navigating new technologies and data privacy

The ICO's tech horizons report 2025 discusses technologies that the ICO thinks are likely to be introduced in the next two to seven years. While not wanting to pre-empt future policy positions, the ICO presents its early view on these highly uncertain, evolving technology areas. Similar technologies are in fact currently being assessed in the ICO's regulatory sandbox.

A part of the ICO's report addresses content partially or entirely generated using AI or machine learning, including images, video and audio. This includes deepfake content which is already a problematic issue and is now included in the Data (Use and Access) Bill which would create new offences in respect of sexually explicit images, produced digitally without consent. While the ICO supports this aim, it also points out that there may be implications for UK EU adequacy if the provisions conflict with the European Convention on Human Rights to which the UK is still a party. Read more about the Data Bill, currently at the House of Commons, on p.1.

The ICO has recently responded to the government's request for plans to secure economic growth (p.22). The area of digital marketing is of great importance to the UK's economy and the stakes are high as organisations are grappling with new cookie developments (p.1 and p.8) as well as 'consent or pay' (p.10). On the EU side, the European Commission has finally given up on the e-Privacy regulations (p.5).

Also in this issue, our correspondent analyses the ICO's guidance on AI tools in recruitment (p.11). Transparency is a key component but how, in practice, to explain use of AI to individuals? (p.14). Lastly, I had the pleasure to interview children's privacy advocate Claire Archibald about her work (p.18). This topical area is also the subject of a *PL&B* conference on 11 March (p.1 and p.21) – I hope to see you there.

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

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 *PL&B* events documentation, except for the 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

"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, Tech, Data and AI Partner, Cripps LLP

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.