Thomson Reuters™

AI, Data and Breaches: Fortifying Personal Data Breach Prevention and Response Processes (UK and EU)

by Kate Brimsted, Partner, Shoosmiths and Practical Law Data Privacy & Cybersecurity

Status: **Law stated as of 11-Mar-2025** | Jurisdiction: **European Union, United Kingdom**

This document is published by Practical Law and can be found at: **uk.practicallaw.tr.com/w-046-0390**
Request a free trial and demonstration at: **uk.practicallaw.tr.com/about/freetrial**

This article highlights the need for customers and suppliers to amend their data breach prevention and response processes when using AI enabled tools and services. It suggests practical steps to protect against heightened and new risks and to maintain compliance with UK and EU data protection regulations through robust safeguards and cooperation.

The integration of artificial intelligence (AI) into corporate operations and supplier services can bring transformative efficiencies. At the same time, AI enabled tools or services can potentially increase existing security vulnerabilities and also present entirely novel security and privacy risks. For example, model inversion attacks can reveal sensitive information, such as indicating that an individual was included in a training data set, which in turn could have serious implications, such as, identifying Alzheimer's patients.

All of this calls for robust safeguards to protect against heightened and new risks. This article suggests some practical steps for customers and suppliers to consider when reviewing their data privacy breach prevention and response processes in response to AI adoption. The steps may also be relevant for security incidents that do not involve personal data. Organizations are likely to deploy AI for both personal and other types of data. Therefore, a useful first step in determining whether a personal data breach may have taken place, could be to analyze whether affected information qualifies as personal data. See Practice Note, Meaning of personal data (UK) and Checklist, Meaning of personal data (UK).

Specific reporting obligations apply in the event of a qualifying "personal data breach", defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Organizations subject to the GDPR or UK GDPR (both controllers and processors) must regularly test, assess, and evaluate the effectiveness of the appropriate technical and organizational security measures they have adopted to protect personal data (Article 32(1)(d),GDPR and UK GDPR). Testing, assessing and evaluating personal data breach response plans fall squarely within this remit. For more information, see:

- Practice Note, Data Security Under the GDPR.
- Implementing Data Security Measures Under the GDPR Checklist.
- Practice Note, Data security under the UK GDPR and DPA 2018.
- Implementing data security measures (UK): checklist.
- Global Cyber Incident Response and Data Breach Notification Toolkit.
- Global Information Security Toolkit.

It is worth keeping in mind that personal data breaches in an AI-specific context may take unfamiliar forms, such as data poisoning, where malicious inputs corrupt the AI models, or model inversion attacks, which can lead to the exposure or loss of personal data used by the AI systems. A hallucination containing inaccurate information about an individual (e.g. a corrupted medical scan) could also be a personal data breach depending on the root cause (that is a breach of security versus a model error). See also Article, EDPB Opinion on AI Models Provides Important Guidance Though Many Questions Remain.

IT supply chains can be notoriously long and complex, and the resulting cyber resilience challenges are the subject of much current

regulatory focus. Another feature of a long supply chain is that "customer" and "supplier" are variable roles. A "supplier" in one context may be the "customer" of a general-purpose AI provider in another; the "customer" of one party, may be the "supplier" of its own customers, and so on. See Controller or processor? (UK and EU): checklist.

This article necessarily offers a simplified view of the environment and concepts in order to highlight some themes.

The Role of the Customer

For a company incorporating AI into its software stack, this will mean revisiting its data breach preparedness, alert escalation and incident reporting processes.

Before any organization looks to test, assess and evaluate the technical and organizational security measures it has implemented, it should be able to demonstrate why it considers the measures are "appropriate". This requires a thorough risk assessment specific to the AI deployment in question, looking at how the AI will be used, the existing controls in place, and identifying any gaps that need to be addressed to mitigate new AI-related risks. One critical component of this process is likely to be a Data Protection Impact Assessment (DPIA); however, there may be additional risk assessments required under legislation such as the EU AI Act. For more information, see:

- Standard Document, GDPR Data Protection Impact Assessment (EU).
- Standard Document, Data protection impact assessment (DPIA) (UK).
- Practice Note, Data Protection Impact Assessments Under the GDPR.
- Practice Note, Data protection impact assessments (DPIA) (UK).
- Practice Note, EU AI Act and GDPR: comparing conformity assessments, FRIAs and DPIAs (EU).

Prior to a risk assessment for any new AI implementation, an organization should ensure it has an inventory of any AI-enabled services already deployed:

- Whether they are in test mode.
- Being used only by specific functions.
- Generally available, for example, as a complementary feature of an enterprise software suite available to every employee.

The results of the risk assessment should usefully inform a review of the company's current incident response processes. Part of an effective, AI-ready incident response plan includes establishing clear processes for identifying AI-novel security breaches and defining who is responsible for handling, managing and reporting them.

It may be challenging for smaller companies to obtain expert AI advice regarding the risks of their intended deployment. Possible sources of expertise they could turn to include European Data Protection Board (EDPB) guidance, UK Information Commissioner's Office (ICO) guidance, academic institutions, industry consultants, professional advisers and associations, and government advisory services. See Practice Note, AI and data protection (UK): Other regulatory and government developments and Children's AI: managing data protection aspects (UK): checklist: Understand and monitor laws, regulations and best practice for more information.

It is also possible to request a voluntary audit by some EU supervisory authorities or the ICO. Available resources can provide valuable insights, and guidance tailored to the specific needs of smaller enterprises are likely to increase over time, for example, the AI Management Essentials tool being developed by the UK Department for Science, Innovation and Technology (DSIT) intended for UK SMEs. See Legal Update, DSIT launches consultation on AI management self-assessment tool.

Additionally, as part of the procurement or vendor selection process, organizations should request evidence from vendors regarding their commitment to privacy by design and data minimization. This could include obtaining model instructions for use that detail how privacy measures have been integrated into the AI systems from the ground up. Such evidence can help organizations assess the suitability of a vendor's product in meeting their data protection and security requirements. For more information, see:

- Data Protection Supplier Audit Checklist (GDPR).
- Standard Document, Data privacy AI software or system assessment questionnaire (UK and EU).
- Data protection supplier audit (UK): checklist: AI, cookies and other technologies.
- Standard Document, AI system procurement: due diligence questionnaire (UK).
- Implementing data security measures (UK): checklist: Data protection by design and default.

The Role of the Supplier

For an AI supplier, managing privacy-related data security risks to its own services or underlying model is paramount. Vendors providing models to customers need to be vigilant in protecting against attacks originating from customers or by bad actors who have compromised the customer's system for example, through stolen customer credentials. This is especially crucial when a supplier's AI tool could reveal personal data if attacked.

Contractual terms can further mitigate privacy risks by mandating that the customer implements specific security measures and adherence to best practice. For instance, contracts can require customers to follow guidelines on secure model deployment, regularly update their systems, and conduct security assessments. The AI vendor may also want to include terms that specify responsibilities in the event of a data breach, ensuring clear procedures and accountability. If there is a potential joint controller relationship (see Joint Controllers), this is essential. For more information, see AI Toolkit (International): Commercial Transactions.

Popular machine learning development frameworks are generally open-source, meaning there is an inherent dependency on a large quantity of third party software needing to be installed. This increases the "attack surface" and therefore the risk profile because vulnerabilities in any of the dependent software can potentially be exploited. To mitigate these risks, suppliers dependent on such frameworks should regularly update their software dependencies, perform rigorous security audits, and contribute to the open-source community by reporting and patching discovered vulnerabilities. (A customer may want to seek contractual assurances to this effect).

In addition, it can be beneficial to suppliers to provide guidelines or controls on the purpose and usage of the models ("instructions for use") to their customers. This can help prevent misuse and ensure that the models are used within a secure and controlled environment. If a new or significantly changed system falls within the scope of a high-risk AI system for the purposes of the EU AI Act, then from August 2026, or for safety systems within Annex I, August 2027, the supplier will be subject to comprehensive transparency and information provision obligations (Article 13, EU AI Act) as well as built-in human oversight capabilities (Article 14). For more information, see:

- Practice Note, EU AI Act: Transparency requirements.
- EU AI Act transparency requirements: checklist.
- Practice Note, EU AI Act: data protection aspects (EU).

Procurement Tips

Collaboration and cooperation between the supplier and customer of an AI system are particularly important for the resilience and security of both parties' systems. Interdependencies may well be greater than for a typical Software as a Service (SaaS) relationship. The data privacy risks are also anticipated to be more reciprocal in nature. See Software licensing and development toolkit.

Joint Controllers

Another incentive for closer cooperation is that the supplier and the customer may be joint controllers from a data protection perspective, depending on the precise system and use case (for example, potentially in a federated learning scenario), leading to shared responsibilities for data protection. In such cases, the obligation to report a personal data breach applies to each joint controller (though joint controllers are required to determine between them which party performs the task), and security measures need to be deployed in a coordinated manner to mitigate risks effectively.

AI Literacy

Training responsibilities and achieving appropriate levels of AI literacy are critical security considerations for both suppliers and customers. Incorporating AI literacy into existing training programs and data breach drills can make these measures more effective and relevant for AI-related security breaches. The vendor's understanding of its AI tool (through development and testing) is likely to put it in a good position to educate its customers so they can enhance the quality of their staff training from both a risk and innovation opportunity perspective. That could roll down into the training that the customer offers its own end user customers. See Practice Note, EU AI Act: AI literacy.

Role of Senior Management

Senior management, including Data Protection Officers (DPOs), need to be well-versed in potential security risks, align organizational structures, and ensure that existing compliance frameworks, including data privacy incident response plans provide sufficient coverage post-AI implementation. The responsibility cannot be delegated to data

scientists or software engineers. For more information, see:

- Global Cyber Incident Response and Data Breach Notification Toolkit.
- Practice Note, Data Protection Officers Under the GDPR.
- Practice Note, Data protection officers (UK).

Supplier and Customer Combined Efforts

The combined efforts of the supplier and customer in managing data security are essential, through:

- Coordinated technical measures.
- Clear contractual agreements.
- Ongoing collaboration.

These efforts can enable both parties to preserve the security and privacy of their AI systems, maintaining trust and compliance with data protection regulations.

Practical Steps to Consider

This table summarizes a number of steps to consider from both the customer and supplier perspective.

Practical step to consider	Customer	Supplier
Before engagement	• Prepare AI inventory of any existing AI systems or tools deployed.	• Deploy privacy by design and data minimization principles in training and development.
Collaborating during the procurement phase and information sharing to support the risk assessments mutually	• Define specific use cases and requirements. • Share relevant data and risk profiles. • Ensure vendor solution is suitable from a risk and performance perspective, taking into account testing and assurance information available.	• Provide expertise and guidance on suitable applications and uses. • Consider conducting joint risk assessments and provide security recommendations for customer. • If customer is proposing a novel deployment, determine whether to conduct bespoke risk assessment or decline to supply.
Determine parties' data protection roles (controller, processor, joint controller)	• Do different roles apply to different activities? • Does customer need to retain control over reporting of privacy security incidents, e.g. if financially regulated?	• Does supplier need to retain control over reporting of privacy security incidents, e.g. if a RDSP (AI-as-a-Service) under the UK NIS regulations?
Including appropriate contractual safeguards	• Ensure clear terms for data protection and security obligations. • Impose training assistance obligation on supplier?	• Agree to contractual terms and provide compliance guarantees. • Consider imposing purpose / use restrictions on customer. • Consider imposing minimum security obligations on customer.
Determining how each party should contribute to the security breach processes of the other **When should one party notify the other of an incident or suspected incident**	• Establish protocols for breach reporting and response, including mutual notification of security incidents and the threshold for these. • Factor in possible serious incident reporting obligations under the EU AI Act for deployers of in-scope high-risk systems.	• Establish protocols for breach reporting and response including mutual notification of security incidents and the threshold for these. • Support breach investigation and mitigation efforts.

Practical step to consider	Customer	Supplier
Defining what a "incident" or "personal data breach" means in the specific AI-deployed context		• Would supplier want customer to notify it of compromised employee credentials in case third party can access model and attack it? • Factor in possible serious incident reporting obligations under the EU AI Act for providers of in-scope high-risk systems.
Internal governance	• Training and policy for employees when using AI tools; for example, avoid higher risk uses and be alert to AI-elevated security risks. • Establish who to report to within organization about AI performance related errors. • If consumer-facing, do existing CRM channels enable potential AI-novel incidents to be picked up promptly for investigation? For example, an AI customer services agent gives out account details for another customer in error.	• Similarly, training is important, as are clear internal incident reporting processes. • Rigorous patching of third party software dependencies where OS ML is baked into service / product for customers.

In addition to being a Partner within the Privacy and Data Team at Shoosmiths, Kate is also a member of the Practical Law Data Protection Consultation Board*.*