Browne Jacobson

A digital marketer's dream and a data protection officer's dilemma

Hyper-personalisation: Key considerations for organisations implementing AI solutions

16 April 2025 Saara Leino

In the saturated world of digital marketing, hyper-personalisation stands out as a vital strategy to reach the right customers for your product.

By delivering highly contextualised advertising, hyper-personalisation offers unique, personalised customer experiences that can significantly enhance business opportunities.

Customers expect more personalised service through different channels and effortless shopping experience with as little friction as possible. This is why the use of artificial intelligence (AI) and hyper-personalisation are growing rapidly.

However, this approach presents notable legal and regualtory challenges, particularly concerning data protection and AI governance.

What is hyper-personalisation?

In its essence, hyper-personalisation involves processing the highly individualised, real-time personal data, including behaviour data of an individual operating on a platform by using AI or machine learning techniques. The processing differs from traditional personalisation firstly by adapting in real-time and secondly by including considerably more data points than traditional personalisation would.

While AI-driven hyper-personalisation offers transformative potential for marketers, it also presents significant risks for the individuals.

When considering hyper-personalisation campaigns, it is crucial to reflect on the potential impact on individuals. The sensitivity of the data is just one aspect; the implications of processing outcomes are equally important. For instance, if hyper-personalisation leads to certain consumers receiving better deals or access to credit, while others are disadvantaged, this could result in legal claims or regulatory enforcement actions. Organisations must be aware of these risks and ensure their AI solutions are employed responsibly to avoid significant legal repercussions.

Hyper-personalisation leverages AI to tailor interactions and experiences to individual users at an unprecedented level. The use of hyper-personalisation might be invisible for the users and hence cause the personal data processing to be more intrusive than individuals. Use of hyper-personalisation involves analysing vast amounts of data, including data types such as browsing behaviour, purchase history, and demographic information, to predict and meet consumer needs in real-time. The technology relies on machine learning algorithms and natural language processing to generate the personalised outputs. The origin of the data used for training, validating and testing the system might be unclear. Organisations must ensure that AI is employed responsibly to mitigate legal and ethical challenges. This includes managing data privacy concerns and adhering to regulations, even when using off-the-shelf products or third-party solutions. All of these are issues that need to be solved and fully understood and handled before hyper-personalisation is implemented.

Data protection

Before any personal data is processed, organisations must carefully select the legal basis for processing personal data. Two primary legal bases under the UK GDPR applicable to hyper-personalisation are consent and legitimate interests.

Legitimate interests may serve as a basis for data processing if the organisation can demonstrate that the processing is necessary for its operations and does not override the rights and freedoms of the data subjects. Direct marketing is an example of processing operations where legitimate interest may be appropriate. To use hyper-personalisation based on legitimate interest, a careful balancing test is needed to evaluate the benefits of hyper-personalisation against any potential risks to individual privacy, or indeed wider harms (e.g. discrimination). Organisations must document their legitimate interest assessments and ensure that appropriate safeguards are in place to protect data subjects.

Another way in which data processing might take place lawfully is where appropriate consent has been obtained from individuals. Consent, as a legal basis, requires that individuals are fully informed about how their data will be used and provide their clear and unambiguous agreement. This approach ensures that users are aware of the hyper-personalisation processes and the extent to which their data will be utilised. There is no valid consent without sufficient transparency; organisations need to communicate the specifics of data collection, usage, and storage in a manner that is easily understandable to the average consumer. Furthermore, consent must be revocable, allowing individuals to withdraw their permission at any time. These factors can sometimes make consent difficult to manage, and organisations may need to think about whether reliance on consent is practical depending on the circumstances.

Transparency is not just a regulatory requirement; it is fundamental in building trust with consumers. By openly communicating the processes and purposes behind data usage, organisations can foster a sense of reliability and safety among their customers. Transparency involves providing clear, accessible information about data collection practices, the types of data being processed, the reasons for processing, and how the data will be protected. Organisations may need to inform consumers about their use of AI algorithms and some thought may be required as to how this can be achieved. Providing insights into how decisions are made, what data influences these decisions, and the potential consequences for the user can empower individuals and enhance their trust in the technology.

Organisations can adopt various methods to achieve transparency, such as detailed privacy notices, just-in-time notifications, and regular updates on data use practices. By ensuring transparency, organisations can mitigate concerns about data intrusiveness and uphold individuals' privacy rights.

AI governance framework

An AI governance framework is essential for any organisation looking to implement AI-powered solutions responsibly, especially if dealing with sensitive data or using AI in ways that can significantly impact individuals. It provides a structured approach to managing AI technologies within an organisation, encompassing policies, procedures, and guidelines designed to ensure that AI systems are developed, implemented, and used ethically, transparently, and in compliance with relevant laws and regulations.

The core components of an AI governance framework include establishing clear ethical guidelines that ensure fairness, accountability, and transparency in AI operations. It also involves defining data management policies that govern how data is collected, stored, processed, and shared, addressing data privacy, security, and consent. Compliance and risk management processes are necessary to ensure that AI systems adhere to legal and regulatory requirements through regular audits, risk assessments, and impact analyses. Transparency and explainability are again crucial, as they ensure that AI systems and their decision-making processes can be understood by stakeholders through clear documentation and explanations.

AI governance is particularly crucial in hyper-personalisation scenarios due to the sensitive nature of the data involved and the potential impact on individuals' privacy and trust. Hyper-personalisation relies on extensive data collection and analysis to deliver highly tailored experiences, and without proper governance, this can lead to privacy violations, ethical concerns, and legal risks. Effective AI governance ensures that personal data is handled responsibly, with robust measures to protect privacy, obtain informed consent, anonymise data where possible, and implement strong security controls. By adhering to ethical guidelines, organisations can prevent biased or discriminatory outcomes, build fair and inclusive AI systems, and gain consumer trust through transparency.

In conclusion, an AI governance framework is essential for managing the complexities and risks associated with hyper-personalisation. By incorporating comprehensive policies and ethical standards, organisations can harness the benefits of AI while safeguarding consumer trust and ensuring legal compliance.

Next steps and conclusions

To address the challenges posed by hyper-personalisation, we suggest a simple six-step approach that organisations can follow to ensure ethical and transparent practices:

1. Define **clear objectives** for the use of hyper-personalisation, outlining the intended benefits and potential risks.
2. Carry out **data protection impact assessment** and other risk assessments to ensure that the risks arising from the hyper-personalisation are identified and mitigated.
3. Establish robust **data management policies** to govern the collection, storage, processing, and sharing of personal data.
4. Implement **consent mechanisms** that are transparent and easily revocable, ensuring individuals are fully informed about data usage.
5. Conduct regular **audits and risk assessments** to identify and mitigate potential ethical and legal issues.
6. Ensure the explainability of AI algorithms by providing **clear documentation** and explanations of decision-making processes.

By following these strategic steps, organisations can effectively manage the risks associated with AI hyper-personalisation, ensuring both legal compliance and consumer trust.

If you are interested in learning more about responsibly managing AI solutions, our firm is here to assist. Our experts can provide comprehensive insights and guidance on successfully implementing a responsible AI governance framework.

Previous

Proposed Omnibus Directive: Looming sustainability crisis for fashion retail and its supply chains

Next

Martyn's Law receives Royal Assent: What does it mean for retailers?

Contents

Contact

Francis Katamba

Partner

francis.katamba@brownejacobson.com

+44 (0)330 045 2725

Related expertise

Advertising and marketing

AI regulation and governance

Artificial intelligence

Data protection and privacy

Data protection for retail