




Hogan
Lovells

GMCQ

The Starting Point for a
Big Data Project: The Privacy
Impact Assessment

Summer 18

The starting point for a big data project: the privacy impact assessment



The era of big data is here. Not only do we generate more data than ever before, we now have the tools to analyse it to make inferences, predictions and even decisions. The use of big data analytics has spread throughout the public and private sectors, with applications in fields as diverse as health, education, financial services, retail, marketing and online services. And though we have yet to see the full potential of big data, it is already proving to be invaluable to businesses, helping to provide services more efficiently, streamlining recruitment and customer onboarding processes and improving the effectiveness of marketing campaigns. However, the use of big data has also been the source of much controversy, particularly where it involves sensitive information, concerns children, minorities or other vulnerable people, or where the decision-making has a significant impact on individuals. As both public interest and regulatory scrutiny in artificial intelligence, machine learning and big data continues to build, it is increasingly becoming important for businesses to be aware of individuals' rights over their data and be prepared to demonstrate compliance with data protection laws.

This is particularly the case for organisations working with data about individuals in Europe, as the regulatory framework on data protection has changed with the EU General Data Protection Regulation (GDPR) coming into force in May 2018. One of the innovations of the GDPR is the introduction of the focus on accountability, which is the requirement to not only comply with the obligations of the GDPR but also be able to demonstrate compliance with the GDPR. The data protection impact assessment (DPIA), also called privacy impact assessment (PIA), is an important tool that organisations have at their disposal to ensure that their processing of personal data complies with data protection law and minimises the impact on privacy. This guide is intended to explain why, when and how PIAs should be carried out in the context of a big data project. It also discusses some of the key issues that are likely to be identified in a PIA on a big data project and factors to consider when making risk-based decisions on the basis of a PIA.

“

One of the innovations of the GDPR is the introduction of the focus on accountability.

”



Why carry out a privacy impact assessment

Big data projects, by virtue of their definition, involve data. Lots of data. Arguably, the most interesting big data projects involve analysing information about people. The big data projects with some of the most valuable applications for companies and public sector organisations alike involve analysing information to make inferences, evaluations and predictions about individuals' preferences, behaviour, performance at work, spending habits, health, location, reliability, the list goes on. The high volume, velocity and variety of the information involved in a big data project means that unless fully anonymised datasets are used, large volumes of personal data will be processed, potentially affecting the privacy rights of the individuals whose data is being processed.

For starters, it is not possible to know whether and how a big data project will impact on the privacy rights of individuals without carrying out an assessment. A privacy impact assessment (PIA) is just that, an assessment of the data flows involved in the project to make sure that the data can be collected, used, processed, stored and shared in the way proposed in the design of the project. If there are any conditions that need to be met or any safeguards that need to be put into place, a PIA will identify them and ensure that the necessary measures are adopted in the project plan. A PIA is also a very useful record that can be used to demonstrate compliance with applicable data protection laws, whichever laws these may be. For these reasons, it is good practice to carry out at least a high level PIA on all projects involving processing of personal data, even when it isn't strictly required by law.

When is it required

Under the EU General Data Protection Regulation (GDPR), there is a new requirement to carry out a data protection impact assessment (DPIA) where a type of processing is "*likely to result in a high risk*" to individuals. The GDPR applies from the 25 May 2018 to all organisations established in the EU as well as non-EU organisations that offer goods or services to individuals in the EU or monitor individuals in the EU.

Just a word on terminology: a DPIA is the same thing as a privacy impact assessment (PIA) in substance, but the GDPR uses the specific term DPIA when setting out the requirement to do one. For the purposes of this article, we will use the term DPIA to refer to PIAs carried out to meet the specific requirement under the GDPR, and PIA as a more general term that includes DPIAs and other assessments carried out more generally.



When considering whether a proposed project is likely to result in a high risk to individuals triggering the requirement for a DPIA under the GDPR, the following ten criteria should be considered:

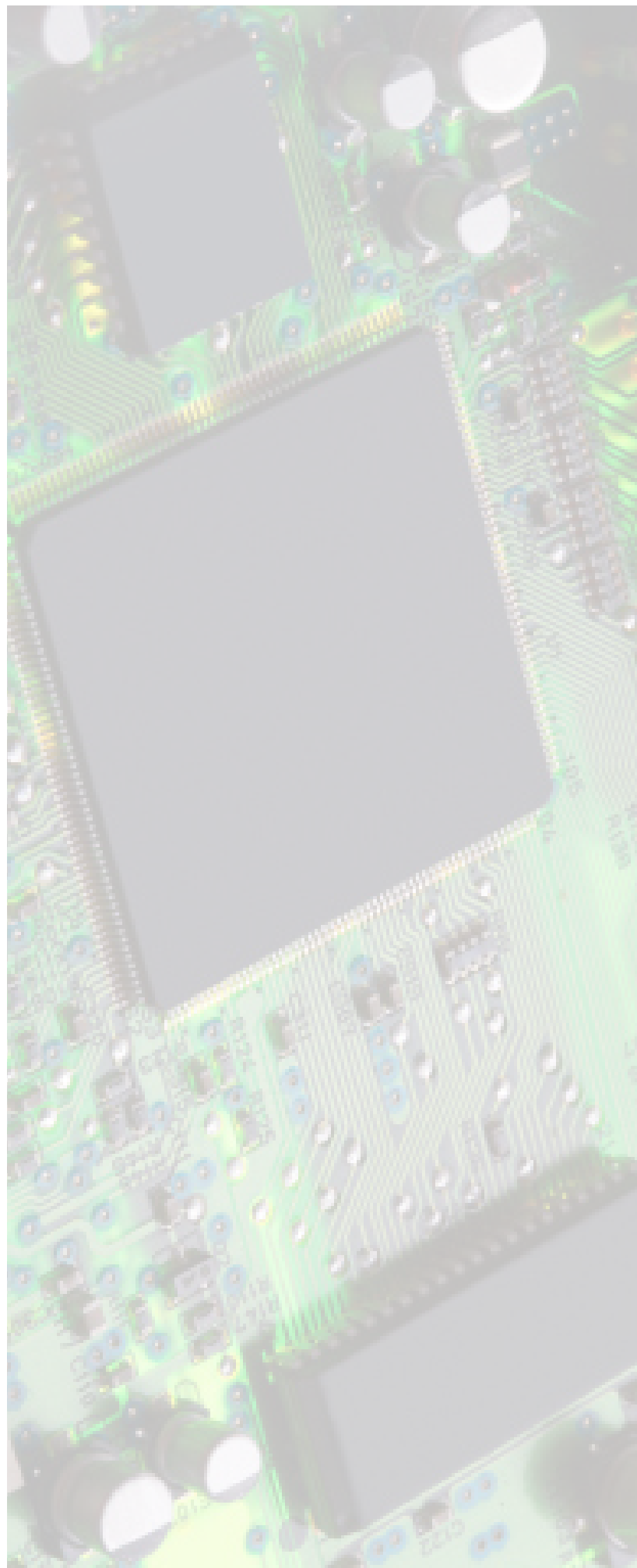
10 Questions: Is the project likely to result in a high risk to individuals?

1. Does the project involve evaluating or scoring individuals, including profiling and predicting aspects about the individual's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?
2. Does the project involve automated decision-making with legal effects (e.g. terminating a contract, denying access to a statutory benefit, etc.) or similarly significant effects (e.g. denying someone an employment opportunity, access to education, eligibility to credit, access to health services, etc.)?
3. Does the project involve systematic monitoring of individuals used to observe, monitor or control data subjects, including data collected through a systematic monitoring of a publicly accessible area (e.g. footfall traffic analysis in a shopping mall)?
4. Does the project involve processing sensitive personal data? Sensitive personal data includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, information about an individual's sex life or sexual orientation and data about criminal convictions and offences.
5. Does the project involve data processed on a large scale, taking into account the number of data subjects concerned, volume of data and the range of different data items being processed, the duration of the processing activity and the geographical extent of the processing activity?
6. Does the project involve datasets that have been matched or combined, for example involving data from different projects set up for different purposes that the individuals involved would not reasonably have expected?
7. Does the project involve processing data concerning vulnerable individuals or individuals in a position of imbalance of power (such as children, the elderly, patients, mentally ill, asylum seekers or employees in the context of human resources management)?
8. Does the project involve a new technological or organisational solutions (such as new Internet of Things devices, use of vision AI such as face recognition or combining existing technologies for innovative solutions)?
9. Does the project involve transferring data across borders outside the European Union?
10. Is the processing of data in the project used to prevent data subjects from exercising a right or using a service or contract? For example, refusing an individual's eligibility to obtain credit, access to a service, entry into a contract or employment?

As a rule of thumb, if the answer is 'yes' to two or more of these questions, the proposed project is likely to present a high risk to the privacy rights of individuals, and so a DPIA will be required to be carried out under the GDPR. Big data projects are likely to meet at least two of the criteria for high risk processing requiring a DPIA in most instances. For example, a project involving gathering information from social media, fitness tracking app usage information, gym access records, and purchasing history from certain retailers to profile individuals' interests, economic status and health to price insurance premiums and offer discounts for certain deals is likely require a DPIA. This is because it would involve (1) evaluation or scoring and (4) sensitive data as well as (6) datasets that have been matched and combined. Another example is a project involving screening CVs and references of job applicants using machine learning algorithms built on an analysis of previously successful candidates. Such a project is also likely to require a DPIA as it would meet criteria (1) evaluation or scoring and (2) automated decision-making.

In some cases, even a project that meets only one of the listed criteria may pose a high risk to the privacy rights of individuals. For example, a smart city project may involve collecting wi-fi signals emitted by mobile phones collected via hotspots throughout the city to understand how many people visit the city, how frequently they visit and how they move around the city. Similar projects may also be carried out at shopping malls, theme parks, music festivals or other venues. Such a project would only involve (3) systematic monitoring of a publicly accessible area, but is likely to result in a high risk to individuals particularly if the movements of the users can be tracked at an individual level, for instance by reference to a device identifier. Given the impact of such monitoring on the individuals' privacy, a DPIA would be required to make sure that safeguards can be identified and put into place.

Even when not required by the law to carry out a DPIA, for instance because the GDPR does not apply to the organisation, it is highly recommended as good practice to at least do a high level review of any big data project to assess the impact of the processing on the privacy of the individuals involved.



How to carry out a privacy impact assessment

Privacy impact assessments should be carried out at the outset of planning for a project, before any processing takes place. A PIA should be an integral element of the project design and development phase, as the ability to collect and process data lawfully is crucial to the viability of any big data project.

In practice, the PIA is usually carried out through completing three types of documents:

1. Preliminary PIA questionnaire.

This document is formulated as a series of questions to obtain information about the project, its purposes and information flows. It is used to make a determination of whether or not a full PIA is required. If it is determined that a full PIA is not required, the responses to the Preliminary PIA questionnaire can be used as a record of the decision not to do a full PIA and a record of processing activities.

2. PIA Questionnaire. This document is formulated as series of more detailed questions about the project to obtain the information necessary to complete a full PIA. Once completed, it is used to carry out a full PIA.

3. PIA Report. The PIA Report identifies the privacy risks of the project and the measures that need to be taken to safeguard individuals' privacy rights, and contains the following information:

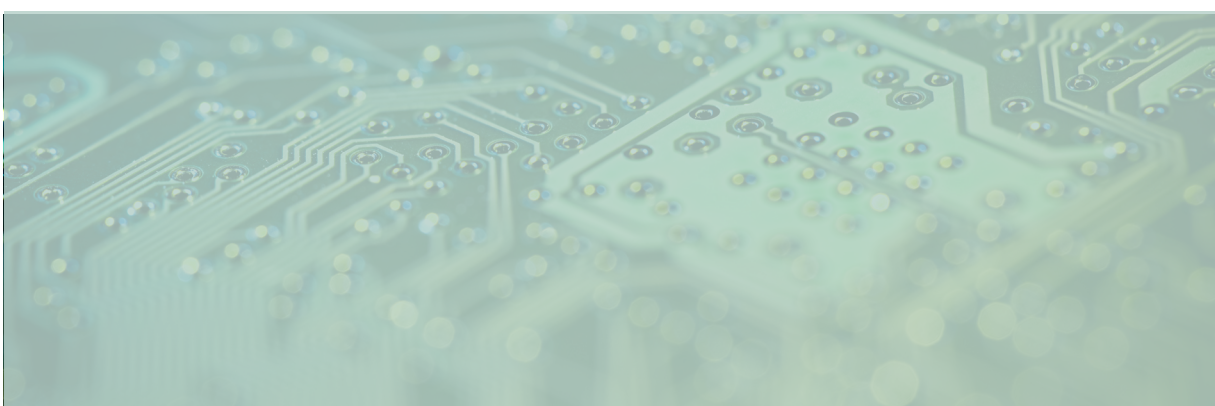
- Description of the envisaged processing operations and purposes of the processing
- Assessment of the necessity and proportionality of the processing
- Assessment of the risks to the rights and freedoms of individuals
- Measures envisaged to address the risks and demonstrate compliance
- Results of any consultation with relevant stakeholders (Data Protection Officer, data protection authorities, data subjects, etc.)

The PIA Report should be kept as a record of the processing activities and as reference for monitoring the implementation of the recommended safeguarding measures.

It is recommended that templates of these three key documents are developed and incorporated into the project development process. Yet, a PIA is more than a document production exercise, and should not be considered a mere formality or box-ticking exercise. The issues identified in a PIA and the recommended measures to safeguard individuals' privacy rights and comply with data protection law needs to be actioned and resolved.

Key issues likely to be identified in a PIA of a big data project

So far, we've gone over why, when and how privacy impact assessments should be carried out. But what will you find out at the end of the PIA process? This of course depends on the project and the applicable data protection laws.



From a GDPR perspective, however, the following are some of the key issues that can be expected to be identified from a PIA on a big data project:

Issue	Risk to individuals	Recommended safeguards
<p>1. Transparency Individuals need to be properly informed about how their personal data will be used</p>	<ul style="list-style-type: none"> In a big data project, there are likely to be complicated information flows with datasets from multiple sources and complex processing activities involving algorithmic and statistic models. Depending on the context of the project, the results from the analysis may reveal unexpected insights into the data that some people might find intrusive or 'creepy'. 	<ul style="list-style-type: none"> It is important that individuals whose data are being used for the project are provided with clear, intelligible information about the how their personal data will be used. The GDPR contains specific requirements about what information needs to be provided to individuals and when it needs to be provided. Measures should be taken to provide appropriate privacy notices to individuals.
<p>2. Lawfulness The processing activity must be lawful, meaning that there must be a lawful ground for processing the personal data and any special conditions must be met if applicable</p>	<ul style="list-style-type: none"> Big data projects are likely to rely on the lawful ground that the processing is in the legitimate interests of the organisation carrying out the project. In such cases, it is important to identify the specific legitimate interests being pursued (e.g. marketing analysis, human resource management, fraud prevention, improved efficiency, etc.) and those interests must not be outweighed by the rights and freedoms of the individual. In some cases, consent from the individual will be required if there is no alternative lawful ground or if a special condition applies, for instance because there is sensitive data involved or there is automated decision-making that has a legal or other similarly significant effect. 	<ul style="list-style-type: none"> The PIA will identify which lawful grounds should be relied on for the particular processing activities at hand. If consent is required, measures will need to be taken to collect valid consent that meets the higher standards for consent under the GDPR. Even if consent is not required, safeguards may need to be put into place to rely on legitimate interests, such as allowing individuals to opt out of the big data project. Appropriate policies and processes will need to be in place to ensure that the project does not experience 'mission creep' where the processing goes beyond what is allowed under the lawful ground being relied on.

Issue	Risk to individuals	Recommended safeguards
<p>3. Purpose limitation Personal data must be collected for specific purposes and used only for those purposes.</p>	<ul style="list-style-type: none"> • Big data projects often take the approach of analysing all of the data that is available, collated from a multitude of diverse sources to create a rich dataset. There may not even be a clear specific purpose at the outset of the project. • This means that personal data may be processed for purposes that are yet unknown and unexpected for the individuals involved. These purposes may also be incompatible with the purposes for which the data was initially collected. 	<ul style="list-style-type: none"> • Make sure that the data used is collected fairly, lawfully and transparently. • Check the privacy notices provided to the individuals at the point of data collection. • Consider whether the analysis is likely to be compatible with the purposes for which the data was originally collected. If not, the individuals will need to be informed. • Consider using anonymised datasets for the initial scoping phase of the project.
<p>4. Individuals' rights Individuals' rights need to be respected and processes must be in place to respond to requests from individuals to exercise their rights.</p>	<ul style="list-style-type: none"> • Individuals have certain rights over their data, subject to local law, including: <ul style="list-style-type: none"> • access • rectification • erasure • restriction of processing • data portability (this right applies only where personal data is processed on the basis of consent or contractual necessity) • objection (where the processing is based on the 'legitimate interests' condition) • certain rights in respect of automated decision-making 	<ul style="list-style-type: none"> • Policies and processes must be in place to respond to requests from individuals to deal with any requests to exercise their rights. • Systems need to be designed so that individuals' rights can be actioned. For instance, systems need to be able to export, delete or rectify data if requested.

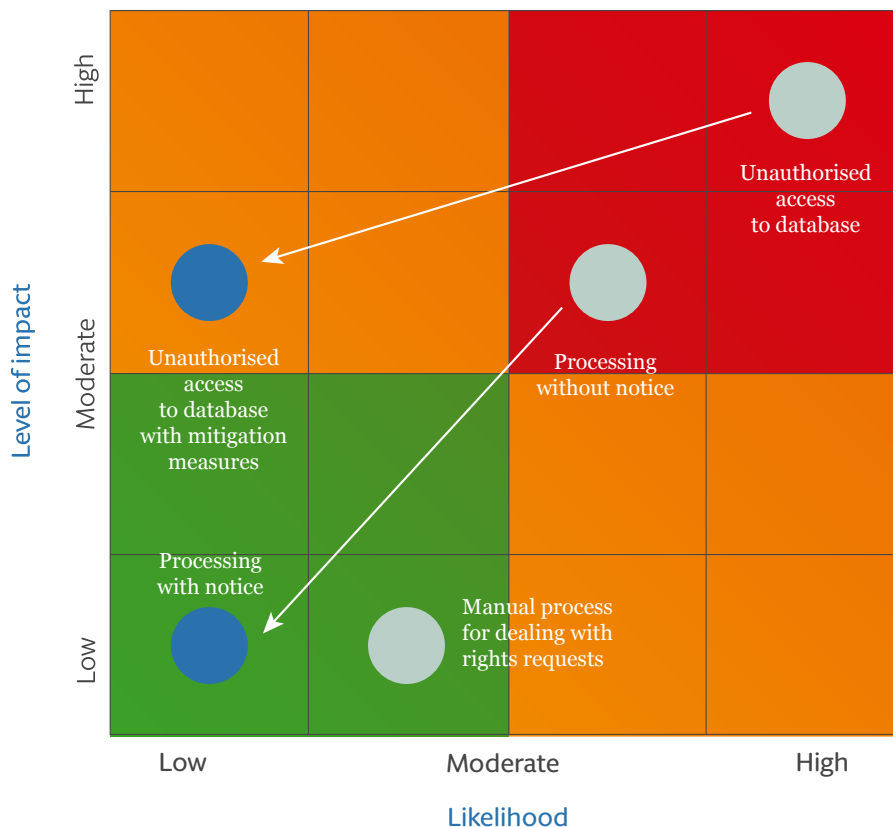
Issue	Risk to individuals	Recommended safeguards
<p>5. Security Personal data must be kept securely and adequately protected</p>	<ul style="list-style-type: none"> As big data projects tend to involve large datasets, it is very important to keep this data protected from accidental or malicious loss. This is particularly important when there are multiple organisations (such as companies, academic institutions, public sector bodies, etc.) cooperating to share their data, resources and expertise, so that data is not compromised in storage or in transit at any of the participating organisations. 	<ul style="list-style-type: none"> Technical and organisational security measures must be in place to keep the information secure. Measures such as encryption and pseudonymisation should be adopted and effective processes should be in place to deal with data breaches. If anonymised datasets are used, regular testing should be carried out to ensure that the individuals cannot be re-identified. Contractual safeguards should also be in place between participating organisations to ensure the division of responsibilities are clearly set out
<p>6. Accountability Organisations must be able to demonstrate compliance with data protection obligations</p>	<ul style="list-style-type: none"> In some big data projects, especially those making use of machine learning using unstructured datasets or other innovative analysis methods, there is a risk that the methods for deriving outcomes are opaque, creating a 'black box' effect. This type of processing can pose particular risks for individuals because it is more difficult to demonstrate that the processing has been carried out fairly and lawfully. 	<ul style="list-style-type: none"> Measures should be in place to ensure that algorithms are auditable. A human review of the algorithm should be carried out to ensure that the approach taken is ethical and non-discriminatory. Algorithmic biases that may lead to direct or indirect discrimination on any protected characteristics must be corrected.

Making risk-based decisions based on a PIA

Once a PIA has been completed, the next step is to decide how to deal with the risks that have been identified. As discussed above, a number of privacy risks are likely to be identified through a PIA of a big data project. Whilst the key principles and obligations in the GDPR provide a regulatory framework through which privacy risks can be identified, the GDPR is largely silent on what constitutes a "reasonable" level of risk to take on a project and what measures are "appropriate" to mitigate privacy risk. For instance, it is evident that a security breach resulting in unauthorised access to the project database which contains information about a large number of individuals is likely to result in a significant privacy risk to the individuals involved. Yet, what is the "appropriate" security measure to take? And as no solution is ever perfect, when does an organisation know that they have done enough, and that the residual risks are "reasonable" to take? The short answer to these issues is that it depends. It depends on the type of personal data, the categories of data subjects, the processing activities, the systems and algorithms used, the measures and safeguards already adopted, the purposes of the project and the risk tolerance and culture of the organisation in question. The GDPR only tells us that the measures must "*tak[e] into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.*"¹ For data protection by design², and security measures³, the GDPR says that measures should also take into account the state of the art and the cost of implementation.

One way to usefully visualise the privacy risks in a project to determine the relative priorities for allocation of resources is through a privacy risk map, which may look like the below:

Example privacy risk map



In this Example Privacy Risk Map, the various privacy risks associated with a project are evaluated on the basis of the severity of privacy impact on the individuals involved and the organisation and the likelihood of the risks arising. The privacy risk map can also track the change in risk profile once mitigation measures are adopted. For example, the PIA of a big data project may identify a shortcoming in the database security system. If this were the case, there would be a high likelihood of unauthorised access to the database. If such a security breach were to occur, this would result in a significant impact to the individuals as well as the organisation concerned. Therefore, this risk would be mapped on the privacy map in the red upper right hand section as shown, and be flagged as a top priority item for remediation. Mitigation measures would be needed to move the risk downward (lower impact) and to the left (lower likelihood) on the graph. Any risk in the upper right hand section of the graph is likely to be considered unacceptable under any circumstances. On the other hand, the PIA may identify as a risk that the only way the organisation can deal with certain individuals' rights requests is by processing them manually. However, based on previous track record, the organisation does not expect a high level of rights requests and is confident that it can deal with such requests as they come in using existing processes and resources. In this case, the risk would be mapped on the privacy risk map in the lower left hand section as shown, with a lower priority for remediation. Other risks can be mapped on the privacy risk map in a similar way.

Even after privacy risks have been evaluated, mapped and prioritised, there is still the question of deciding what measures are "appropriate" to reduce the level of risk to an acceptable level. A common sense approach to this question would be to balance the costs and efforts of implementing safeguards against its obligations to protect the privacy of the individuals involved. The level of mitigation measures adopted should be proportionate to the likelihood and level of impact of the risk – the bigger and more likely the risk, the more robust the safeguards. That much is obvious, and uncontroversial.

However, measures taken to mitigate risks may be costly. The most significant cost will often be the reduced utility of the data processing brought about by the mitigation measure. This is especially true in big data projects where the obvious mitigation measure – anonymize the data – may significantly reduce the value of the insights derived from the data. To reach an acceptable level of risk, and determine what level of mitigation measures are "appropriate", we contend that a key factor to consider is the underlying purpose and the expected social welfare resulting from the project, and how the mitigation measures may affect that social welfare.

The U.S. Federal Trade Commission ("FTC") has developed a similar methodology to determine whether a data practice is "unfair" and therefore prohibited by Section 5 of the FTC Act. The FTC developed explicit guidelines to help make its methodology for judging "fairness" more transparent and predictable by businesses. A business practice is considered unfair if it causes substantial injury to consumers that consumers cannot reasonably avoid, and the injury is not offset by corresponding consumer benefits. In other words, the practice would be prohibited as unfair if and only if:

$$H - H_A > W_A - W_P$$

Where:

H is the total aggregate consumer harm created by the practice

H_A is the aggregate harm that consumers can reasonably avoid

W_A is the total consumer welfare when the practice is allowed

W_P is the total consumer welfare when the practice is prohibited

How is this formula relevant in the context of assessing privacy risk mitigation measures under the GDPR? To bring this formula to life, let's take two different types of hypothetical big data projects:

- **Project 1:** A visual AI pilot project involving handheld devices carried by visually impaired individuals in a national museum to provide real-time feedback about the exhibition and the people around them
- **Project 2:** A visual AI pilot project involving digital billboards installed in shopping malls that analyse passers-by's fashion trends and shopping bags to display real-time custom advertisements of available products and offers

Both projects involve similar technology (i.e. visual AI) and process similar types of personal data (i.e. biometric information, information about the behaviour of individuals, etc.) about similar categories of data subjects (i.e. individuals in public places) with similar risks to individuals' privacy (i.e. individuals in public places may not wish to be filmed with visual AI technology analysing them). Let us assume that on an initial PIA of both projects, it has been identified as a risk that the individuals who are being filmed and analysed are not given appropriate notice of the processing taking place. If these projects were to proceed without proper notice, the practice would be in breach of the transparency obligations of the GDPR. Yet, when deciding how to provide the notice and accepting any residual risks if a pragmatic solution is adopted, an analysis based on the formula above can be useful, as below:

	$H - H_A$ (total aggregate consumer harm created by the practice) – (aggregate harm that consumers can reasonably avoid)	$W_A - W_P$ (total consumer welfare when the practice is allowed) – (total consumer welfare when the practice is prohibited)
Project 1	<ul style="list-style-type: none"> The harm (H) created by the project proceeding without proper notice would be that individuals visiting the museum may be filmed and analysed through visual AI technology without their knowledge. In particular, the museum may be visited by children. Without proper notice of the processing activities, visitors to the museum will not be able to avoid being subject to the processing or to object to the processing. To avoid the harm, visitors would have to refrain from visiting certain parts of the museum, which is not a reasonable avoidance mechanism. H_A would therefore be zero. 	<ul style="list-style-type: none"> The benefits of the project would be greater accessibility of cultural and educational centres to visually impaired people to encourage them to visit and navigate the premises independently. The success of the pilot programme could be an important precedent for similar programmes in other public places improving access for visually impaired people. If this project were not to proceed, this would limit the way new visual AI technologies could benefit visually impaired people.
Project 2	<ul style="list-style-type: none"> The harm created by the project proceeding without proper notice would be that individuals visiting the shopping mall may be filmed and analysed through visual AI technology without their knowledge. In particular, the shopping mall may be visited by children. Without proper notice of the processing activities, visitors to the shopping mall will not be able to avoid being subject to the processing or to object to the processing. Let us assume that as in Project 1, H_A would be zero. 	<ul style="list-style-type: none"> The benefits of the project would be more effective on-premise digital billboard marketing for shopping malls. The data collected through the digital billboards can be used to analyse fashion trends, shopping habits and popular brands to maximise the effectiveness of marketing campaigns. The project could also help shopping mall visitors find the products and offers that are more relevant to them effectively. If this project were not to proceed, this could limit the effectiveness of offline in-premise marketing campaigns

“

As public awareness and interest in big data, artificial intelligence and machine learning heightens, it will become increasingly important to build relationships of trust with the public.

”

The net harm analysis is very similar for both projects: the harm is that visitors could be filmed and analysed without their knowledge, and the harm cannot be easily avoided by visitors in either case. However, the benefits analysis is different. On the one hand, Project 1 has a public policy benefit as it has the potential to improve access to public places for visually impaired people that would have a significant positive impact on their quality of life and opportunity. On the other hand, Project 2 has a commercial benefit that would improve the effectiveness of marketing campaigns and improve profitability of the participating companies.

For both projects, the solution is clear: individuals need to be given notice of the processing so that they can reasonably avoid the harm if they wish. With appropriate notice, the benefits of both projects would outweigh the harm. But given the different benefit profiles of the two projects, it is arguable that the measures that need to be taken to provide this appropriate notice is different, as below:

- For Project 1, it may be sufficient to provide a prominent notice at the entrance of the museum about the project with information about how to get in touch if there are questions or concerns. The handheld devices can also be of a prominent colour, with a light indicating when it is in use, so that it is clear when they are being used. Given the benefits of this project, it is arguable that such measures would be enough to provide a reasonable level of notice.

- For Project 2, a similar approach may not be sufficient. In addition to a notice at the entrance of the malls, additional notices may need to be served at each digital billboard. It may also be a reasonable safeguard to calibrate the digital billboards such that only the people who step inside a clearly delineated space are subject to the analysis and profiling, so that people can easily avoid those spaces if they wish.

To put it simply, given the different societal benefits in the two projects, the level of "appropriate" technical and organisational measures may also be different. Members of the public will be more accepting of such pilot programmes to improve access for visually impaired individuals. Though this doesn't exempt Project 1 from privacy considerations altogether, it means that in practice, people are less likely to object or complain about the processing, which gives more leeway when making risk-based decisions on specific safeguards to be adopted. In contrast, though Project 2 is not without its benefits, people are more likely to view visual AI and profiling for marketing purposes to be more intrusive. Given the high numbers of complaints regulators receive about direct marketing, a pilot programme like Project 2 is likely to result in more complaints and regulatory scrutiny than Project 1. With this in mind, it is advisable to take a more circumspect approach to providing appropriate notices and general data protection compliance for Project 2.

At the end of the day, privacy is an intangible and in most cases immeasurable right. How people feel about privacy is often based on emotions and subjective evaluations about the trade-offs involved. Privacy risks that are acceptable for processing for a certain purpose may not be acceptable for another purpose. Risk mitigations measures which are reasonable for privacy risks in one context may not be appropriate for another context. This is what makes carrying out PIAs so critically important for any project that involves the processing of personal data, and especially big data projects. The PIA is one of the most important tools that organisations have at their disposal to ensure compliance with data protection laws, as it provides a framework for identifying the risks and the specific safeguards to be adopted. The PIA will start with a description of the anticipated benefits associated with the project, both commercial benefits and broader societal benefits. A clear identification of the benefits will help gauge the level of mitigation measures necessary to address each risk. Each mitigation measure should be evaluated based on its effectiveness in reducing the risk, but also based on its impact on the benefits anticipated from the project. A mitigation measure may be extremely effective, but if it destroys half the utility of a big data project, it may be excessive and therefore not "appropriate".

As public awareness and interest in big data, artificial intelligence and machine learning heightens, it will become increasingly important to build relationships of trust with the public. Ensuring that personal data is processed fairly and lawfully, respecting individuals' choices and keeping them informed are crucial for both public acceptance and compliance with evolving data protection laws. The PIA is the key for identifying the specific, practical steps that must be taken to achieve this aim. We suggest that the PIA should clearly identify the benefits associated with a data project so that risk mitigation measures can be evaluated with the benefits of the project in mind.



Sam Choi

Associate, London
T +44 (20) 7296 5756
sam.choi@hoganlovells.com



Winston Maxwell

Partner, Paris
T +33 1 53 67 48 47
winston.maxwell@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

“Hogan Lovells” or the “firm” is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word “partner” is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2018. All rights reserved. 1025702_0818