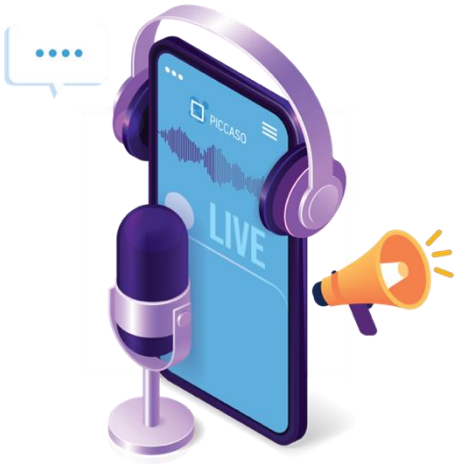
PICCASO

Privacy & Security Insights with PICCASO



Assessing the Assessments

Robert Bond

Solicitor, Notary Public and Compliance & Ethics Professional

The Data & Marketing Commission

Sponsored by

PrivacyCulture

Assessing the Assessments

"The value of risk assessments in the world of data protection compliance"

In the world of data protection, we have grown used to, or even grown tired of, the requirement to carry out a Data Protection Impact Assessment (DPIA) or a Privacy Impact Assessment (PIA) as it is called in some jurisdictions.

What are PIA and DPIA?

They are processes that help assess privacy risks to individuals in the collection, use and disclosure of personal information. They identify privacy risks, improve transparency and promote best practice.

In a report by Trilateral Research & Consulting, commissioned by the ICO in 2013[1], it was recommended that "Ensuring the "buy-in" of the most senior people within the organisation is a necessary pre-condition for a successful integration of privacy risks and PIA into the organisation's existing processes. PIA processes need to be connected with the development of privacy awareness and culture within the company. Companies need to devise effective communication and training strategies to sustain a change in the mindsets of, and in the development of new skills for, project managers. The organisation needs to deliver a clear message to all project managers that the PIA process must be followed and that PIAs are an organisational requirement. Simplicity is the key to achieve full implementation and adoption of internal PIA guidelines and processes.
The GDPR and guidance from Data Protection Authorities make it clear that projects that may require a PIA include:

- A new IT system for storing and accessing personal data;
- Using existing data for a new and unexpected purpose;
- A new database acquisition
- Corporate restructuring
- Monitoring in the workplace

A DPIA will become mandatory in the following cases:

- Systematic and extensive evaluation of personal aspects of natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects on the individual or similarly affect the individual
- Processing on a large scale of special categories of data or data relating to criminal offences
- Systematic monitoring of publicly accessible areas on a large scale

Some data protection authorities have published guidance on how and when to effectively use a DPIA and the DPIA process is best broken down into several distinct phases which are:

- Identify the need for the project to have a PIA
- Describe information flows
- Identify privacy risks
- Identify privacy solutions
- Record outcomes and obtain sign-off
- Integrate outcomes of PIA into project plan

But it is not as simple as set out above

My experience is that if a DPIA is a risk management tool and is to be considered at the outset of a project, then almost every project or new processing activity needs a pre-DPIA screening process.

[1] https://ico.org.uk/media/1042196/trilateral-full-report.pdf

This at least flags up if a full DPIA is needed and will highlight any areas of risk. These risks may not only relate to possible infringements of fundamental rights but also to business and reputational risks and infringements of other laws.

Assuming that a full DPIA is needed then it is not long in the process before we are assessing the lawful grounds for processing and if we are relying on Legitimate InterestS then we need to do a Legitimate Interests Assessment.

Legitimate Interests Assessments (LIAs) – the "balancing test"

An essential part of the concept of Legitimate Interests is the balance between the interests of the Controller and the rights and freedoms of the individual:

> *'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a Third Party,* ***except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of Personal Data****, in particular where the data subject is a child.'*[2]

If a Controller wishes to rely on Legitimate Interests for processing Personal Data it must carry out an appropriate assessment, called a Legitimate Interests Assessment, or LIA. When carrying out an LIA, the Controller must balance its right to process the Personal Data against the individuals' data protection rights.
In certain circumstances an LIA may be straight forward. However, under the accountability provisions of the GDPR, the Controller must maintain a written record that it has carried out an LIA and the reasons why it came to the conclusion that the balancing test was met.

International Data Transfer Risk Assessments

In so many projects and data sharing activities we find that personal data is being transferred and the EDPB guidance on risk assessment[3] must be followed and for Controllers in the UK then the ICO guidance applies. There are six steps:

The six steps:

Note that, in order to meet the GDPR's accountability requirements, each of these steps would need to be documented, and the documentation provided to the supervisory authorities on request.

Step 1: Know your transfers
Understand what data you are transferring outside the EEA and/or UK, including by way of remote access. Perhaps fairly self-evident, but can be challenging when it comes to onward transfers by processors (to sub- processor, or even sub-sub-processors).

Step 2: Identify your transfer tool(s)
Identify what lawful mechanism you are relying on to transfer the data.

Step 3: Assess whether the transfer mechanism is effective in practice
Now we come to the crucial question: in practice, is the transferred personal data afforded a level of protection in the third country that is essentially equivalent to that guaranteed in the EEA/UK?

---

[2] GDPR Article 6(1)(f)
[3] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

The EDPB recommends considering multiple aspects of the third country's legal system, but in particular the rules granting public authorities rights of access to data. Most countries allow for some form of access for law enforcement and national security, and so the assessment should focus on whether those laws are limited to what is **necessary and proportionate in a democratic society**.

If, after this assessment, you decide your transfer mechanism, ensures an equivalent level of protection, you can stop there. If, however, you decide that the local law does impinge on the protection afforded by your transfer mechanism, you must proceed to Step 4.

Step 4: Adopt supplementary measures
The EDPB separates potential supplementary measures into three categories: technical, contractual, or organisational.

Step 5: Procedural steps if you identified any supplementary measures
This step may lead you to impose regular audits on the importing party.

Step 6: Re-evaluate at appropriate intervals
Monitor developments in the recipient country which could impact your initial assessment. The obligations on the data importer under solutions like the EU Standard Contractual Clauses should help here, as it is required to inform the data exporter of a change of law which impacts its ability to comply with the SCCs.

AI, analytics and new technologies

The EU AI Act is intended to apply to any business that puts AI or uses AI on or in the EU market and so is extra-territorial in its reach. More than that, the AI Act will integrate with and co-exist alongside existing legislation such as the General Data Protection Regulation, the Digital Services Act and the draft Cyber Resilience Act.

The use of new technologies such as smart devices, internet of things and artificial intelligence, coupled with the economic and humanitarian uses of big data analytics, means that there has to be a balance between the acquisition of personal data and the rights of citizens.

Beyond GDPR, PECR, Digital Services Act and so on, assessing your supply chain is more important now than ever, particularly as we rely so much on international suppliers and distributors as well as physical and digital supply chains. We have learned to address issues in the supply chain, such as bribery, competition, modern slavery, and intellectual property; however, more recently we have had to consider geopolitical issues, import and export controls, and other compliance and ethics issues. Now in 2024, we must also consider environmental, sustainability, cyber resilience, digital safety, and accessibility of physical products and digital services that we provide.

Harmful Design in Digital Markets[4]

- This position paper by the ICO and the CMA is targeted to firms that deploy design practices in digital markets (such as on websites or other online services), as well as product and UX designers that create online interfaces for firms. It provides:
- an overview of how design choices online can lead to data protection, consumer and competition harms, and the relevant laws regulated by the ICO and CMA that could be infringed by these practices; and

- [4] https://www.drcf.org.uk/publications/papers/ico-cma-joint-paper-on-harmful-design-in-digital-practices

- practical examples of design practices that are potentially harmful under our respective regimes when they are used to present choices about personal data processing. These practices are "harmful nudges and sludge", "confirmshaming", "biased framing", "bundled consent" and "default settings".

It now needs us to assess how we manage Data Protection by Design and how we respect consumer choices. Yet another assessment to minimize potential risks!

6 years on from the General Data Protection Regulation, we now face a growing list of assessments that we need to carry out, from Legitimate Interest Assessments, Transfer Risk Assessments, Privacy by Design Assessments, Accessibility Assessments, Children's Code compliance, and now Online Safety, AI and Cyber Resilience....and the list goes on. Have we reached the point where we need an Assessments Handbook that incorporates these various assessments I have outlined and ensure they integrate with each organisations overall risk management policy?

Used appropriately, I find that these assessments really do manage risk and not only protect the rights of individuals but also protect the business from reputational and brand damage. Sometimes, the use of a risk assessment at the start of or even at an early stage of a project, can act as a "Stop" sign and cause the project team and compliance team to say "just because we can doesn't always mean we should".

Introduction

Now that the COVID-19 pandemic is behind us, society has begun to live like we did before the fear, isolation and lockdown. Many of us are returning to work from the office, some taking a hybrid approach, and others opting to solely work from home. Whilst some organisations have downsized their office space and others haven't, largely we are witnessing businesses attempting to encourage collaboration and general presence within the office. Despite this, it has been difficult to foster a culture where all employees are willing to return to work from the office as we once did. Subsequently, businesses using monitoring techniques are having to re-evaluate how they monitor and enforce office attendance versus privacy, legal and ethical obligations.

Legal Perspective on Privacy

Just as would be required for any personal data processing, an employer would need to comply with data protection law: the GDPR, UK GDPR and the Data Protection Act 2018. The first step is to identify the lawful basis for processing. The employer must identify whether they can rely on a legal obligation, entering into a contract or legitimate interest (balanced against the employee's rights) for their employee monitoring. Consent almost certainly could not be relied on due to the employee – employer relationship and the superior and influencing position the employer is likely to have.

The next stage is to ensure the processing is fair. The employer will need to consider whether their monitoring activity of choice is proportionate and necessary for the purpose of monitoring employee attendance and obedience to newly set rules to be present in the office. This includes avoiding excessive data collection and ensuring its accuracy. The employer must also ensure that they are transparent about their practices through a privacy notice or alike, and that they do not retain the data collected longer than is necessary and data is stored securely.

Organisations that have received an enforcement action or monetary penalty have quite often failed to achieve this fairness and proportionality test. For instance, when the ICO issued an enforcement notice against Serco Leisure in February 2024 to stop processing biometric data of employees for the purpose of attendance checks and subsequent payment of employees, it did so because Serco failed to show necessity and proportionality. It was commented by the UK Information Commissioner that "Serco Leisure did not fully consider the risks before introducing biometric technology to monitor staff attendance, prioritising business interests over its employees' privacy".

Another example, the French Data Protection Authority (CNIL) imposed a fine of €32 million on Amazon France Logistique for 'excessive' employee monitoring in its warehouse in December 2023. CNIL found that Amazon disproportionately required staff to use scanners to collect and monitor their activities, leading to several complaints. Amazon was in breach of the data minimisation principle, lack of lawful basis and lack of transparency.

It is easy for employers to remember these considerations when it comes to consumers or clients because of the fear of reputational damage or financial loss, however it is vital that employers see their employees' rights equally as the consequences will more or less be comparable.

Employment regulation

Beyond compliance with privacy law, employers will need to consider labour laws and regulations, which may differ depending on the sector and role. It is important that the employer involves privacy, advisers within human resources or an employment lawyer to ensure they have properly considered all angles.

The Challenge

For employers, using monitoring technologies to verify employee attendance may be essential for many reasons, for some this may be to improve productivity, to assist with planning or reprimand for absenteeism. However, no matter the benefit of the monitoring, it is likely to have drawbacks such as decreasing morale, promoting mistrust and in some circumstances reduce job satisfaction. These factors mean it is vital that the employer not only complies with the law, but it must also consider all appropriate factors. This can include the benefits and weaknesses mentioned above and more, but also ethical considerations such engaging employees and maintaining a culture of trust, the size of the organisation and the difficulty of pleasing many people, openness through policies and processes in place (or should be in place), as well as generally seeing their employees as people seeking to live out their rights and freedoms.

Failing to properly consider the challenges presented by employee monitoring and the need to get the right balance and fairness could be an enormous mistake. Employees are the backbone and stronghold of a company, ensuring its operations run smoothly and effectively. Their dedication and hard work can drive the success and growth of an organisation. Monitoring without transparency, thought and consideration could result in the departure of dedicated and or the top achieving workforce, and not to mention significant fines from data protection authorities. In contrast, maintaining a good workforce established on an environment and ethos of trust, transparency and balance; will not be perfect, but the probability of success is likely to be greater and likely to result in no complaints leading to investigation by the regulator.

Balancing Act

Overall, it could be argued that employee monitoring is a balancing act. Data protection law does its best to help employers consider this balancing act and maintain respect and privacy between the employer and employee. It can be a difficult job for the employer to challenge their actions against the employee in the same way they would challenge their behaviour towards a client or consumer. However, if an employer can get the balancing act right, considering as many factors as possible, they could achieve a monitoring system which does not have a huge negative impact or adverse bearing on employee privacy.

PICCASO

Listen now on:

Spotify

YouTube

Apple Podcasts

About us:

We are a UK based non-for-profit privacy special interest group, led by seasoned volunteers who are senior leaders in privacy and data protection.

The primary aim of PICCASO is to create a community of professionals that share the value of exchanging 'know how', insights, clarity and explanation on specific privacy and data protection topics designed to distinguish between legal requirements, operational implementation, and strategic objectives, with the aim of greater understanding in how to achieve optimal outcomes based on good practice and thought leadership.

The PICCASO community is drawn from across the UK, Europe, and beyond, and from all industry sectors.

Contact us:

www.piccaso.org
Bouverie House | 154-160 Fleet St | London | EC4A 2DQ
T. +44 (0) 207 112 9360 | hello@PICCASO.org
https://www.linkedin.com/company/piccaso/