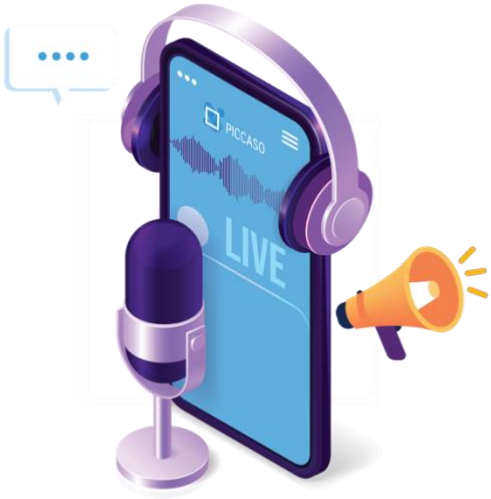
PICCASO

Privacy & Security Insights with PICCASO



Data Privacy Risk – How To Navigate The Complexities

Nick Graham

Partner, Dentons

DENTONS

Sponsored by

PrivacyCulture

Data Privacy Risk - How to Navigate The Complexities

Nick Graham is a Partner in the Privacy and Cybersecurity group at a global law firm, Dentons. Nick is based in Dentons' London office and regularly advises on data privacy risk management. In this article and the associated podcast, we explore privacy risk management, the current landscape, and insights into available tools as well as the PICCASO Privacy Risk Assessment Methodology released in November 2023.

What is Data Privacy Risk?

Data privacy risk is, primarily, about the increasingly prevalent sets of legal obligations and rules that define legal duties and "trip wires" for organisations that process personal data. Obviously, that is pretty much all businesses, public bodies, and other organisations). The growth of new legislation has been both "vertical growth" where the depth and granularity of rules have expanded, as well as "horizontal growth" where comprehensive privacy laws have been adopted by an increasing number of countries worldwide. In 2011 there were 76 countries with comprehensive data privacy laws whereas in 2023, this number has risen to 162 with 20 bills pending[1].

But it is not just about "black letter law". It is also about a basket of related factors such as market practice, local regulatory and enforcement risk, and even local culture. Then there is, what I call, "GDPR fluidity" where there are different interpretations as to what the rules mean in practice. The fluidity risk can be critical as there are lots of examples of the "goalposts moving", even where the legal rules apparently stay the same. Think about cookie banners and the presentation of options! This makes for significant business and operational risk. Businesses will likely want to stay "in the herd" (not outside it whether ahead of it or behind it) and build trust with customers to limit the risk of becoming a target for scrutiny or enforcement action. As you can see, this is a complex picture. We have not even mentioned those very large GDPR fines!

Suffice to say that where data privacy (data protection) used to involve elements of "nuance", in trying to apply the rules meaningfully, we seem to have come full circle. We now have much more detailed rules post-GDPR and yet, a greater need to interpret the nuance to make sense of the risk position.

Impact of technology

In addition, we need to consider the impact of technology in relation to personal data processing. It is not "news" to say that technology underpins this whole area. Software and systems/technology allow enormous volumes of data to be processed and enriched at a very granular level and transferred, pretty much instantaneously, around the globe. The advent of generative AI has (and will continue to) increase the potential of processing power. With this power comes the data privacy overhead of ensuring that you comply with the rules, but also that you demonstrate compliance. This is an underlying principle of GDPR and many similar global data privacy laws.

So, data privacy risk is very real, and the challenge is as to how to best assess it, score it and/or manage it. Organisations have every incentive to do so but the real challenge is as to what methodology or toolkits are available to make this a reality.

Privacy risk landscape

In terms of what is out there, there is no single "gold standard" in terms of methodology or toolkits. In fact, the area has evolved from a traditional approach to a much more complex one. I would see the traditional approach as comprising policies, procedures, audit, training, and awareness. All good stuff! But even when this was talked about pre-GDPR, the practical application was highly variable. Some organisations implemented this in detail. Others selected elements only: for example, measuring timing for responses to DSARs or logging data breaches. Sometimes, this was because they were pushed to do so by a regulator like the ICO. Needless to say, many organisations did not do any of this. What happened in the run-up to GDPR was that organisations wanted to prepare for the Accountability Principle. So, putting in place some sort of control framework quickly became essential but with little or no time to test it out.

Current risk management frameworks

Before generating a new framework or trying to develop your own, it makes sense to look at what is available in the market. There are a number of competing frameworks that you could use either as published or selecting elements to include in your existing internal framework or internal audit procedure. In the UK, for example, there is the ICO Accountability Tracker with a long list of very detailed requirements, organised by risk area. However, many organisations will either select elements from it or adopt certain components only as it is (and this is not a criticism) the superset of requirements. It makes sense, after all, that you choose the elements that are relevant to your business, types of data, sensitivity, and risk appetite. It is undoubtedly better to have implemented key elements of privacy risk management effectively. Trying to do everything at once may be simply too much for certain organisations to support.

It is also worth looking at the NIST Privacy Framework which has a creative process-focussed methodology encouraging organisations to consider a superset of exemplar practices for privacy risk management, a target profile (ie. where the organisation would like to be on privacy risk) and a current profile (ie. where it currently is). The framework also describes Implementation Tiers as a point of reference on whether the organisation has sufficient resources/agility to manage the risk. There may well be elements of the NIST framework that organisations could usefully adopt or re-purpose to fit with the way they operate.

PICCASO PRAM: a new methodology

In November 2023, PICCASO launched its Privacy Risk Assessment Methodology. This was an initiative of PICCASO Privacy Labs where an industry-leading working group of DPOs and privacy law experts contributed practical tips on how to measure and manage privacy risk. The output was a white paper, including insights and how to manage data privacy risk, as well as a toolkit of metrics, and risk management controls (including a heat map). In addition, it was recognised that often the DPO will need a short set of questions to test current compliance quickly, perhaps after recently joining an organisation, but to do so in a controlled and systematic manner. The toolkit therefore includes DPO Triage Questionnaire for this purpose.

Other reference points for frameworks

In addition to the classic control frameworks, you also have alternative models such as the EU Certification schemes (Privacy Seals) such as Euro privacy. It is fair to say that Privacy Seals are still at an early stage, but it is worth noting that Euro privacy, in particular, cites a helpful and very detailed set of "what good looks like" in terms of privacy compliance. It also includes subject-specific sets of requirements relating, for example, to video cameras and audio monitoring, IoT, smart cities, biometrics anonymisation and AI, as well as connected vehicles.

Also, there are the EU Binding Corporate Rules referential tables. These set out requirements that should be addressed in BCR applications. But you could also use the referential (the updated BCR-C ones were adopted in 2023 and we are currently waiting for updates for the BCR-P one). These are intended to underpin the BCR approval process but could be used to "kick the tyres" and help inform good practices on privacy compliance.

International

This is an inevitable risk that an international organisation is subject to different laws in different countries and that these rules likely overlap or conflict or, perhaps, simply expand the total sum of law, guidance and associated nuance (let's call it the "privacy aqui") required to assess and get comfortable with data privacy risk. Even within the EU bloc, there are material variations (of course permitted by GDPR) by individual member states. Similarly, as our US team regularly remind us, there are many US State laws relating to privacy and this inevitably creates risk, even within a single country like the USA.

One way to resolve this is first, to identify jurisdictions where your organisation triggers local data privacy laws. This is likely to be on the basis of local "touch points": (i) establishment or services directed at a jurisdiction; or, in some cases (ii) simply processing data about individual's resident in that jurisdiction. Having identified the active risk jurisdictions, there is another challenge which is to identify how to "bolt together" the various legal requirements in these jurisdictions so as to create a single set of rules and procedures/protocols. One way to do this is to batch jurisdictions into separate benchmarks. In other words, each jurisdiction in the organisation's footprint will be assumed subject to framework components reflecting: (i) GDPR; (ii) GDPR (modified – same but without all the rights if not required); (iii) CCPA (the US is a different model); and (iv) other cases (perhaps China). This way, you can ensure that the input requirements to your framework (and the same works with the PICCASO PRAM toolkit excel spreadsheets) are measurable in a consistent and coherent fashion.

What about the future?

One of the challenges is in tracking and keeping up to date with global laws that encroach onto data privacy issues but sit outside the traditional data privacy frameworks. Look, for example, at the plethora of tech laws in the EU with the AI Act, the DSA, DMA and NIS 2. Along with the need to consider these other laws, is the need to be cognisant of the greater diversity of regulators paying close attention to data privacy. For example, the UK's Digital Regulation Cooperation Forum (DRCF) brings together four regulators: the Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO), the Office of Communications (Ofcom) and the Financial Conduct Authority (FCA).

More generally, there is little doubt that we are going to continue to see more data privacy laws and enforcement. I think there will be continued growth in standards and Privacy Seals as there will also be pressure to deliver privacy risk management in a cost-efficient and effective manner.

So, it is a business regulatory and operational priority to actively manage data privacy risk and ensure that you have a process (methodology, control framework and toolkit) that underpins this. Equally, there is a need to be pragmatic and focus on "real world risks" as this will be the way to get C-suite attention and really "move the needle". Equally, while this still feels like the start of the conversation on what "good looks like", it is a much a better idea to get going with something, rather than thinking it is all too difficult. Time to get moving. We'd be very interested in your feedback and comments.

References

[1] Privacy Laws & Business International Report February 2023: Global Data Privacy Laws 2023: 162 national laws and 20 Bills (Graham Greenleaf)

Listen now on:

Spotify

Google Podcasts

YouTube

Apple Podcasts

About us:

PICCASO is a UK based global facing 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/