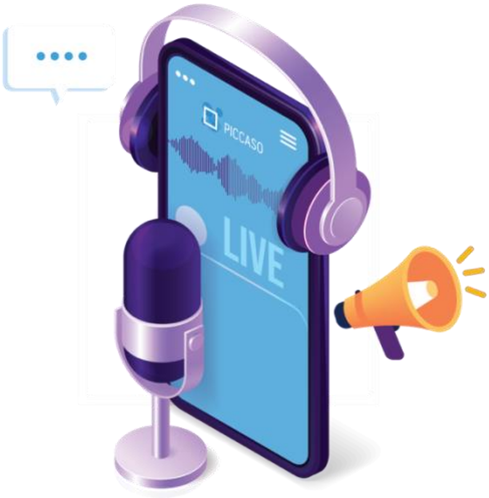
PICCASO

Privacy & Security Insights with PICCASO



Generative AI & Data Privacy

Graham Hunt, Director

Natasja Pieterman, Data Privacy Lead

Capgemini

Sponsored by

PrivacyCulture

Generative AI & Data Privacy

How easy does it seem to put a few key words into a system browser and a whole story comes rolling out? As a matter of fact, we could have asked ChatGPT (a version of Generative AI/GenAI) to write this article. Seems like everywhere you go people are talking about GenAI. Whether it's the next best thing since sliced bread or a precursor to the apocalypse. But what is GenAI? Why is it different from AI? And how should it be considered from a Data Privacy perspective?

What is GenAI?

Think of it in the same way we would describe a mobile phone 30 years ago compared to now. Whatever we think GenAI is now will change. In straightforward terms, it is what it says on the tin: AI (Artificial Intelligence) software that is used to generate content - written or spoken words, pictures, music, even objects (think 3D printing).
Here is a comparison:

If you are a lawyer, you may use AI currently to help scan vast amounts of Legislation and Case Law for specific documentation related to a requirement. It will list the material and may even assign a level of relevance or priority. If you use Generative AI, you could do exactly the same thing, but "ask" the routine to provide a summary of the Regulation and Case Law. It will then write ("generate") a summary of the aggregated data. Further, as the requests come in, the AI will "learn" and refine the summaries it provides.

Benefits vs Risks

GenAI can benefit society in many ways, and most large organisations are spinning up GenAI initiatives. However, the disclosure of data to AI tools can also create risks. As a Privacy practitioner, it's best to get in from the ground up.

Benefits for Data Privacy

As a Privacy Professional, you can help your organisation protect its personal data through GenAI. An example is in the ability to create synthetic data. Often in organisations, we struggle to get data sets to be able to test new services or products. Fed the right parameters, anonymised data can be readily created. Another example is in the medical profession. We already are seeing its use to create synthetic jaw x-rays for trainee dentists. "Real" x-rays can be deemed personal data, but a trained GenAI routine can easily create the equivalent synthetically. This is just touching the surface of what GenAI will be able to do.

The Concerns and the Controls

Where Personal Information has to be used, here are some of the top concerns in controlling GenAI:

- There has to be a purpose – why is personal data being used and has it gone through an impact assessment?
- How to we anonymise?
- Do we have consent?

- Where is the data is stored? Make sure you know where that data resides and who it resides with;
- Can the data be deleted? - How long is the shelf life? Are Retention periods known and advertised? And are retention periods even possible? As GenAI learns from the underlying data, that input cannot be easily removed;
- Who owns it? – If things go wrong who needs to care about fixing it?
- Who looks after it? – once its build, how will the GenAI routines be monitored?
- How does it work? – Can the GenAI application functionality be explained?
- Can we live without it? If it stops working, or has to be stopped, can we cope?
- Data Loss – Are processes in place to deal with incidents if the GenAI Solution leaks Personal Information?
- Finally, are these questions built into the DPIA and Privacy by Design principles of our organisation?

There are great opportunities for organisations when it comes to GenAI, but without the right protections the dream can become a real nightmare.

Listen now on:

Spotify

Google Podcasts

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/