Privacy policy principles: Gen's recommendations

As businesses, public administrations and citizens meet never ending challenges to protect personal data, Gen has put together the following fundamental privacy policy principles to help them successfully safeguard the privacy of individuals. These principles are not to be seen as an exhaustive list but rather as some key principles that are actionable and aimed at ensuring secure data protection and privacy. This comes at a time when risks by technologies, business practices and individuals' use of online applications and services continue to increase.

Privacy policy principles for companies and public authorities

Building upon its commitment to fair and ethical handling of consumer data, Gen has formulated the following principles that are to be adhered to and implemented by any business that considers itself privacy-focused and has an ambition to process personal data of its consumers responsibly. While nearly any business should be able to comply with the following, some may want to go even further in their privacy focus.

The principles below that are also generally applicable to public authorities aim at helping organizations to process personal data of individuals responsibly and ethically.

Take appropriate security measures to protect personal data

Companies and public authorities should take appropriate security measures to ensure personal data is kept safe and secure. While there is no one-size-fits-all approach, organizations must duly analyze their information security landscape, take measures that are optimal in their circumstances and regularly update them.

Improve the use of straightforward privacy notices to increase transparency

Privacy policies should be written in clear and easily understandable language. Companies should make it easy for people to understand the impact of their choices. One of the ways to achieve it is to provide short just-in-time privacy notices at the very moment the individual is taking an action resulting in some change as to the way their personal data is processed.

Minimize the amount of stored data

Companies and public authorities should minimize the amount of data they store and process to the absolute minimum needed to achieve the purpose of processing. This is the easiest way to limit risks associated with data breaches.

Consumer-centric data processing

Companies should not process personal data in a way that would be detrimental to the interests of their consumers and society and should evaluate actual impacts of the processing on the wellbeing of the consumers

Avoid behavioral manipulation

Companies should not use private information they learned about their consumers to manipulate their behavior and should avoid the use of dark patterns in their products.

Privacy by design should be at the center of public authorities' actions

Public authorities should lead by example and embed privacy considerations into all of their processes, operations and technologies from the outset. To the maximum possible extent, legislation or government orders should go through a Privacy Impact Assessment. The principle of privacy by design obviously also applies to companies, but the public sector appears to be far behind the business in this respect.

Privacy policy principles for people

In addition to privacy principles to be adopted by companies and public authorities, individuals themselves should take responsibility for protection of their own privacy and consider adopting privacy-protecting behaviors. These actions might entail getting informed on data control and related rights, thinking before clicking and sharing and adopting basic security practices. Examples include antivirus tools, password hygiene or secure online payment to name a few.

Gen takes the opportunity to remind people that:

- Many businesses nowadays offer various ways in which they can control their data. People should familiarize themselves with the options offered by the businesses they interact with and **adopt settings that are most privacy-preserving**.
- **Being mindful that what is on the internet once is on the internet forever.** Think about this before posting or sharing anything online, especially any personal or sensitive information.

Gen, a global tech leader

Gen is a global cybersecurity leader, with dual headquarters in Tempe, Arizona and Prague, Czech Republic. The company marks its presence in over 150 countries, catering to nearly 500 million customers worldwide. The Gen portfolio includes comprehensive cybersecurity solutions from a family of trusted brands such as Norton, Avast, LifeLock, Avira, AVG, ReputationDefender, and CCleaner.

Digital Freedom as a key principle

Powering Digital Freedom lives at the heart of everything Gen does. This goes beyond the company's mission to create solutions that enable people to navigate their digital lives safely, privately, and confidently. It's about empowering both the generations of today and future generations to be able to take advantage of the ease technology offers, worry free. That's why Gen approaches everything we do with the customers and communities we serve in mind. We champion the simplification and safeguarding of customer experiences in the ever-evolving digital landscape, reinforcing our role as a leader in digital security and empowerment.

If you want more information, please reach out to: Kim Allman, Head of Corporate Responsibility, ESG & Government Affairs (kim.allman@gendigital.com)

Transparency Register number: **083146048556-68**

United States: 60 E Rio Salado Pkwy STE 1000 Tempe, AZ 85203
Czech Republic: Enterprise Office Center Pikrtova 1737/1A 140 00 Prague 4