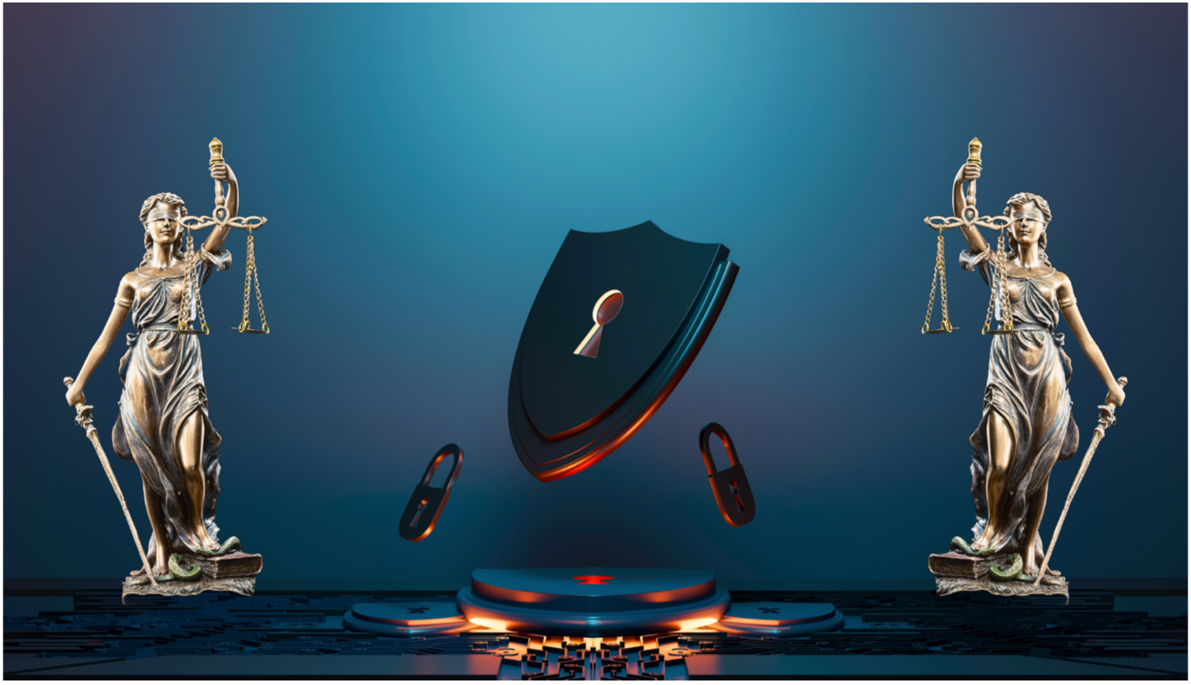
Data Privacy Awareness Campaigns – Shifting the Paradigm: Stop talking about fines and start talking about human rights

Written by Joshua Bucheli, Talent Community Manager at cyberunity AG



In the ever-evolving digital landscape, executives are increasingly tasked with safeguarding their organizations against an array of digital threats. They continually stress the importance of data privacy, emphasizing that *all* employees must be active participants in the battle for secure information. This emphasis on awareness and participation is key, however, there is room for improvement when it comes to messaging.

Awareness campaigns often centre around company reputation, bureaucratic protocols, compliance with new regulations and potential fines. But these are not the things that data privacy is ultimately about, and it's high time that its true core is brought to the forefront of the corporate agenda: data privacy is a *human right*. Employees must be made aware that it is not merely a corporate concern, but an essential aspect of their own personal rights and freedoms – only then, will they reliably play their part in upholding data privacy in the workplace.

A Corporate Concern?

The concerns of executives around corporate data privacy awareness are certainly well-founded. Data has become one of the world's most valuable assets, and handling it responsibly is essential for the continuity of any business – after all, there are crippling, potentially even fatal regulatory consequences for companies that handle data inappropriately.

The messaging aimed at employees when it comes to rallying them around this new concern often emphasises the repercussions a company can face in the event of data leaks and breaches, which include financial penalties and reputational damage. While these aspects are critical and provide a strong incentive for compliance from a corporate perspective, they tend to obscure the fundamental reason for data privacy regulations: protecting the rights and freedoms of individuals. As such, they do little to motivate employees to navigate the proverbial minefield that is data privacy.

As is often the case, different interest groups care about different things, and when they do care about the same thing, they often have different reasons for doing so. If you want an audience to care about something, it may seem reasonable to present the reasons why you care about it. But a much more effective approach is to find out why *your audience* should care about it, and present those, much more convincing arguments. Corporate data privacy awareness campaigns remain far too focused on the former rather than the latter, and it is therefore not surprising that companies are struggling to get employees involved in the fight for data privacy.

A Fundamental Human Right

Data privacy is not just a matter of corporate compliance. It is, first and foremost, a matter of human rights. The right to privacy (both digital and analog) is enshrined in numerous international documents, such as the UDHR (Art. 12), the EU's CFR (Art. 8), the ICCPR (Art. 17) and the GDPR. These documents affirm that individuals have the *right* to be protected from arbitrary or unlawful interference with their privacy, family, home, or correspondence. In today's digital world, this includes the safeguarding of personal data from unauthorized access, theft, or misuse.

The fundamental concept behind data privacy is therefore the autonomy of individuals over their personal information. It's *primarily* about having control over what data is collected, how it is used, and who has access to it, *not* about companies avoiding fines or reputational damage. This concept is not only a matter of legality but a matter of ethics.

With this in mind, it becomes obvious that data privacy is much more than just a mundane administrative chore – it is an embodiment of our basic rights in the digital realm. For corporations, this means that fostering a data privacy-aware culture will require a shift in perspective.

Instead of framing it solely as a compliance issue, companies will need to emphasize that data privacy aligns with the fundamental rights of their employees. It's about empowering individuals to have control over their digital identities and the information that comprises them – not about avoiding fines.

Educating and Empowering Employees

The foundation of an effective privacy-awareness campaign lies in understanding that data privacy isn't merely about safeguarding information, or one's employer; it's about preserving an individual's autonomy and dignity in the digital sphere. Every click, swipe, or online interaction generates a digital footprint—a unique fingerprint that encapsulates an individual's preferences, beliefs, and behaviours. Respecting data privacy means safeguarding these personal facets from unauthorized access or exploitation.

To foster a culture of data privacy and security within an organization, it is crucial that employees be empowered with knowledge about their rights and the ethical principles underpinning data privacy. This knowledge goes beyond mere awareness of the potential consequences of data breaches; it extends to understanding why privacy regulations exist in the first place. Imagine if managers only respected labour laws for fear of punitive corporate fines, rather than a recognition of the basic rights that these laws protect.

Employees need to recognize that they aren't just protectors of company data and their employer's reputation; they are champions of their own rights. When data privacy becomes synonymous with personal empowerment, engagement in safeguarding information becomes a matter of personal responsibility rather than a mandated obligation.

Corporations who want their employees on side in the fight for privacy compliance will find much more success if they emphasise the connection between data privacy and individual rights, making sure that employees understand *why* they should respect privacy protocols before training them on *how* to do so.

How might this look in practice?

1. **Educate on Fundamental Human Rights**: Organizations can incorporate human rights education into their cybersecurity and privacy training programs. Employees need to know that data privacy regulations are not arbitrary rules conceived to make their lives difficult but are grounded in fundamental human rights and represent a cornerstone of free and democratic societies. By framing the discussion in this context, employees are more likely to perceive data protection as a shared responsibility and may be more inclined to take pride in defending this right for themselves and others

2. **Promote Ethical Responsibility**: Companies can encourage employees to view data privacy as a matter of ethical responsibility rather than just corporate compliance, emphasising the moral duty of respecting the right that individuals have to privacy. This perspective can instil a deeper sense of purpose in protecting data, beyond the fear of penalties or damage to an employer's reputation.

3. **Empower with Control**: Corporations may want to consider providing employees with a sense of control over their own data, encouraging and equipping them to actively manage their own privacy settings, both at work and in their personal lives. This hands-on experience can help sensitise individuals to the importance of the privacy of others in their daily interactions with technology.

4. **Open Dialogues on Ethical Dilemmas**: Employers can also create a space for open discussions about ethical dilemmas related to data privacy, motivating employees to explore the complexities of balancing privacy rights with the need for security and transparency. Engaging in these conversations can help employees better understand the nuances of data protection. Practical examples and case studies can illustrate how data breaches or unauthorized access impact not just the company but also the individuals behind the data. Interactive workshops and real-life scenarios can highlight the potential consequences of overlooking data privacy. Employees need to understand that data breaches can lead to identity theft, financial loss, or even

emotional distress, emphasizing the direct impact on real lives

By grounding data privacy awareness trainings in this context, corporations can engender a more profound sense of accountability and commitment among employees. This approach doesn't merely create compliance-oriented behavior but fosters a culture where individuals *proactively* champion data privacy and protection, recognizing it as an extension of their own autonomy and dignity.

Ultimately, data privacy is not a matter exclusive to cybersecurity executives and compliance officers. It is a human right that should be understood and upheld by every individual within an organization. While the fear of regulatory fines and reputational damage can drive compliance from a corporate perspective, the true foundation of data protection lies in everyday employees playing their part – something that will only happen if they understand that individual autonomy and rights are at stake.

Only by embracing this ethos can companies foster a culture where data privacy isn't a burden, but a shared responsibility aligned with the core values of respect for individual autonomy and dignity in the digital age. And yes… this will also help them avoid fines.