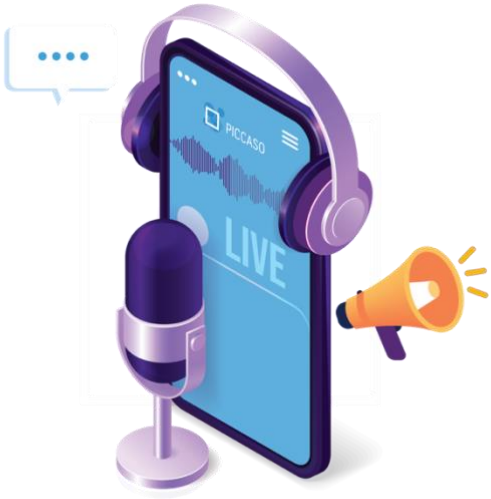
PICCASO

Privacy & Security Insights with PICCASO



Measuring the Effectiveness of Privacy Regulation

Steve Wright, CEO and Founder

PrivacyCulture

Sponsored by

PrivacyCulture

Measuring the Effectiveness of Privacy Regulation

Measuring the effectiveness of privacy regulation is crucial to ensure that the intended goals of such regulations are being achieved and that individuals' privacy rights are adequately protected.

Effectiveness can be assessed through a combination of qualitative and quantitative methods, and it may involve evaluating various aspects of privacy regulation.

The most crucial element to measuring the effectiveness of privacy regulation is the circumstances or environment in which the privacy regulation or compliance objectives are being implemented. Most organisations have common functions and business operations, but each has their own staff – which in turn brings a difference in culture, attitudes, and behaviours.

This is where measuring can come unstuck, as measuring from one division to another or measuring across differing jurisdictions can be tricky and the results can vary significantly.

Therefore, it becomes important to ensure regional or functional variations are considered or variances allowed for when establishing your measurements of effectiveness in terms of privacy regulation.

Take productivity as an example. The UK* has a significantly lower productivity rating per capita than France, Germany, and the USA. However, if you apply different measurements, you can see an entirely different set of figures. In other words, it is very difficult to apply the same comparisons between one organisation and another – and the same can be said for measuring one country against another country.

This means that you need to be careful when setting up your measurements, and to build into your calculation method a certain level of variance or adjustment, given the local environment where you are implementing the privacy regulations. The more obvious [1]example is like comparing 'retail shop outlets' to 'manufacturing car parts'. There is little point trying to compare like-for-like in these scenarios.

Therefore, when considering your measurement (or metrics) or control framework (as it is often referred to), it is important to consider the environment, culture, and metrics to be used. Certain metrics can also be misleading, consider Data Subject Access Requests as a measurement. Would this be an appropriate measurement for our Car Parts Manufacturer? No, because how many customers would be making such enquiries, or requests, very few I suspect.

So, we need to be thinking more about SMART objectives - Specific, Measurable, Achievable, Relevant and Time-bound, taking into consideration the environment, the nature of the organisation's business and the culture of the organisation. Some organisations would adopt metrics or measurements depending upon their sector or culture i.e., a heavily regulated industry like banking, that is used to working with specific controls and within regulatory constraints.

[1] The Economy Enquiry 2030 – Resolution Foundation: https://shorturl.at/fuyH0

Measuring the effectiveness of a control objective is also another good way to accomplish your 'effectiveness'. Thinking more about people and process rather than reporting on policy

compliance. This allows greater flexibility on what you measure, how the control is perceived, and crucially - what risks a control is mitigating. Another factor is if the control is not operating effectively, then it cannot effectively manage the risk to ensure that it does not fall foul of the privacy regulation.

So, in order to test the control effectiveness, the organisation must seek to answer two questions: i) have the controls been designed effectively, and ii) is the organisation operating these controls effectively?

Although this can appear straightforward, there are many pitfalls when designing and implementing effective controls that should be considered. More mature organisations will understand the cost of running and assuring a control and be able to compare it to the reduction in risk and incidents. They are then able to perform a cost-benefit analysis for their controls.

Below are some example ways that can be used when building your privacy regulation effectiveness measurements:

1. Compliance and Enforcement:

- Assess the level of compliance with privacy regulations among organisations. This can involve conducting audits, surveys, or spot checks to identify violations.
- Evaluate the effectiveness of regulatory bodies in enforcing privacy regulations, including the number of investigations, fines imposed, and the speed of enforcement actions (e.g. Review NYOB enforcement data).

2. Data Breach Incidents:

- Track the number and severity of data incidents and breaches before and after the implementation of privacy regulations. A reduction in the frequency and impact of breaches can be an indicator of effectiveness.

3. Consent and Transparency:

- Analyse the extent to which organisations provide clear and understandable privacy policies and obtain informed consent from individuals for data processing activities (e.g. check your cookie and marketing consent methods).
- Conduct staff culture surveys or end-user focus groups to gauge people's awareness and understanding of their privacy rights and how their data is being used.

4. Individual Empowerment:

- Measure the ease with which individuals can exercise their privacy rights, such as the right to access their data or request its deletion (e.g. Mystery shopper enquires via Customer Services).
- Evaluate the effectiveness of mechanisms for individuals to report privacy violations or seek recourse, such as complaint mechanisms and ombudsman offices.

5. Impact on Business Practices:

- Assess how privacy regulations have influenced the business operations, including changes in data collection, storage and processing procedures (e.g. Data Governance frameworks/ Procedures).

- Examine the adoption of privacy-enhancing technologies and practices across IT and business operations (e.g. Data Lifecycle & Records Management, Encryption adoption rates).

6. Economic Impact:

- Analyse the economic impact of privacy regulations on your businesses, including compliance costs, job creation or loss, and changes in market dynamics (e.g. use the IAPP publications on cost of Privacy to help calculate your costs).

7. Public Perception and Trust:

- Measure public trust in you brand and organisation regarding data privacy, both before and after the introduction of privacy rules and regulations. Obviously, this is tricky if you are not starting from scratch.
- Monitor public sentiment and media coverage related to privacy issues (Sources: NOYB, CMS Tracker, IAPP, PICCASO).

8. Cross-Border Data Flows:

- Evaluate the impact of privacy regulations on international data transfers in the context of your organisation, including how to navigate global data protection requirements (e.g. Data Flows, ROPAs, TIA registers, Third Party Contracts).

9. Data Privacy Impact Assessments (DPIAs):

- Assess the extent to which your organisations are able to efficiently conduct DPIAs to identify and mitigate privacy risks associated with their data processing activities. Track this through to mitigation and consider its relationship with the wider Enterprise Risk Management schema.

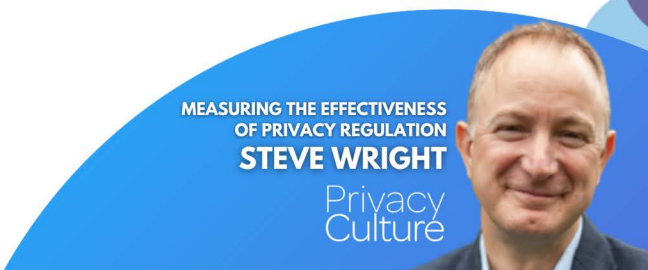
10. Long-Term Outcomes:

- Consider the long-term impact of privacy regulations on societal values, data protection culture, and the evolution of technology and data practices across your organisation, especially pay attention to jurisdictions which have evolving data protection regulation.

Conclusion

It's important to note that measuring the effectiveness of privacy regulation can be complex and multifaceted – in other words, be prepared to get help, outside counsel and take your time to get them right. It may even require collaboration between regulatory authorities, academic researchers, industry stakeholders, and civil society organisations. There are a variety of comprehensive data sources, but not all of them are accurate. Additionally, the effectiveness of privacy regulation may evolve over time as technology and societal norms change, making ongoing assessment and adaptation of regulations necessary, so as to make sure that this features part of your metrics and monitoring activities as you embed and operationalise your privacy program.

Steve Wright



PICCASO

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/