Assurance Reporting for Privacy and Data Protection

A drive to privacy and data protection assurance

Since the General Data Protection Regulation* (GDPR) came into force, the regulatory regime has developed its expectations that organisations will implement comprehensive data protection controls within their businesses. The UK's Information Commissioner previously stated that: **'…this next phase of General Data Protection Regulation* (GDPR) requires a refocus on comprehensive data protection – embedding sound data governance in all of your business processes.'**

Organisations that are service providers are also facing increased expectations from their business customers to provide evidence that their data protection controls are operating effectively. In addition, a heightened level of adverse scrutiny from data protection regulators, privacy activists, citizens and the judicial community is driving the demand for assurance.

Obtaining assurance helps you understand whether your data protection controls have been designed appropriately and are operating effectively. It goes beyond demonstrating compliance through paper-based solutions and requires evidence that compliance is taking place at the operational level, particularly in the people, technology and data layers of your organisation.

Assurance reporting can provide you with an opportunity to demonstrate that purposeful and sustainable data protection outcomes are being delivered within these layers. It can also help drive transparency and trust in how personal data are being processed within your organisation.

Demonstrating appropriateness of design and operational effectiveness of your privacy and data protection controls

The value of assurance reporting

Going beyond the paper layer

Demonstrates that your controls are going beyond the documents you have created and are operating effectively within the people, technology and data layers.

Complying with your commitments

Evidences that your contractual obligations to business customers are being satisfied and that the commitments made to regulators (e.g. in Binding Corporate Rules) are being met.

Challenging your controls

Identifies any gaps in the operational application of your data protection controls and where to apply remediation efforts.

Competitive advantage

Demonstrates the strength and robustness of your data protection controls compared to your competitors, providing you and your stakeholders with increased confidence.

Reduced requests from third parties

Provides interested third parties with an independent assurance report on a subject matter that is of significance to them. In turn, this can reduce audit requests and disruption to your business.

Demonstrating data protection is taken seriously

Shows third parties relying on the report (such as regulators and your business customers) that fulfilling data protection requirements is important to your organisation.

Showing a good risk management system

Demonstrates a good system of risk management and internal controls to address important societal issues relating to privacy. This can aid effective corporate governance and promote the long-term sustainable success of organisations and contribute to wider society.

What is assurance reporting?

Assurance reporting is an independent assessment of the suitability, design and operational effectiveness of an organisation's privacy and data protection controls.

It can either be for a company's internal use (private reporting) or for reliance by external stakeholders such as clients and business customers (public reporting). Where reporting is for the benefit of external stakeholders, this is performed under the AICPA SOC 2 reporting framework.

A SOC 2 report provides an independent assurance opinion covering controls relevant to security, availability, processing integrity, confidentiality and privacy (the 'Trust Service' Principles). It is performed under a rigorous assurance standard, ISAE 3000, and covers multiple areas of an organisation's control framework, from system and environment description to design suitability and operating effectiveness.

pwc

*Regulation (EU) 2016/679

Our approach to assurance reporting

Stage 1

Determine the scope of your assurance report

We work closely with you to scope a tailored assurance report. We take into account the factors unique to your organisation, what it wants to achieve and its priorities.
Our approach includes determining:

- the 'users' of the report, those stakeholder groups that will be relying on your report;
- the products and services in scope;
- the commitments made to the users with respect to data protection; and
- the controls that you have developed to deliver on those data protection commitments.

Stage 2

Assess your readiness for formal assurance

Next, we carry out a readiness assessment for you which serves as a dry run for formal assurance. We will work with you to identify the controls that are meaningful to your users and to determine gaps in your controls that require remediation. You will get a comprehensive report which identifies the controls in scope and the remediation required, equipping you with the understanding to take remedial action and proceed to formal assurance reporting.

Stage 3

Undertake formal assurance and reporting

Depending on the results of your readiness assessment and the needs/timeline of the users of your report, we will either conduct (i) a point in time review that focuses on the design of your controls (known as a Type 1 report); or (ii) a review over a period of time that focuses on both the design and operational effectiveness of controls (known as a Type 2 report). These reports each result in a formal assurance opinion, signed by PwC, demonstrating the robustness and rigour of the reviews undertaken and a means to share the associated comfort over the control framework with both internal and external stakeholders.

Why PwC

Market leaders

We provide assurance reporting to the world's largest organisations and are UK market leaders in control reporting. We are the only firm with a large scale, global Trust & Transparency practice as part of their Assurance offerings.

Data protection controls experience

We have worked with a large number of organisations to design and implement data protection controls. We implicitly understand the challenges of embedding controls into organisations. Our experience and industry insights will guide us in applying the appropriate level of challenge to your controls and ensure that your remediation efforts are focused in the right areas.

Journey to Code

PwC is leading the thinking on how privacy principles can be embedded within systems, processes and controls. As part of this we have developed an indicative privacy controls library which map GDPR articles to controls and to SOC 2 principles.

Data protection compliance experience

Our data protection team has delivered GDPR Readiness and Completeness Assessments to over 250 organisations, providing crucial insight into how to address the risks posed in the 'live' GDPR environment.

Multidisciplinary team and global network

We offer legal, assurance and consulting operational expertise in data protection across a large number of jurisdictions within our international network of firms. We are also able to draw on the experience of a full range of PwC specialists from different disciplines (such as privacy, data, forensics and cyber security) as core members of the team.

PwC's Data Protection team

We have one of the UK's largest data protection teams. We have been recognised for excellence in data protection in legal directories such as Chambers and the Legal 500.

If you would like a conversation on this topic, please contact:

Tim Clough
Partner

E: timothy.clough@pwc.com
M: +44 (0)7483 378386

James Drury-Smith
Director

E: james.drury-smith@pwc.com
M: +44 (0)7841 803538

190610-154634-SP-OS