46

A next-generation privacy framework

Examples in action and precedents

vodafone

Introduction

The principles of European data protection provide a sound foundation for regulation. But economic, societal and technological changes have brought to light fundamental shortcomings: Our regulatory model is inflexible, overly process-oriented, and heavily reliant on legal formalities. It overly burdens stretched national governments, puts European businesses at a competitive disadvantage, and fails to achieve real privacy protections for European citizens.

Industry must do better at respecting consumer privacy. But the regulatory framework must create the right incentives for it to do so. Personal information is essential to the information economy, but the European regulatory framework as it is cannot ensure sustainable economic development or even keep pace with protecting the rights of individuals.

Accountability must be an alternative to prescriptiveness, not an overlay.

We cannot overstate the importance of accountability to improving industry's privacy and data protection performance. Accountability – the outward demonstration of responsibility – has a very important part to play in encouraging the creation of internal governance and assurance processes that deliver better privacy outcomes. But these processes will develop only when they are a substitute for and not an overlay to a prescriptive, legalistic compliance regime.

We explain here how a principles-based accountability model – using many of the features of the existing regulatory framework (codes of conduct, certification schemes and privacy impact assessments) and combined with strong and effective enforcement – can build a solid ground within a next-generation privacy framework.

Accountability is not a new concept, and the challenges faced by policy makers in the privacy sphere are not necessarily unique. Policy makers here can learn from other sectors, such as corporate governance or environmental regulation, so we discuss some precedents that can help guide this Regulation.

How do we build a better Regulation?

To address the shortcomings of the Directive, the Regulation must be reoriented towards a principles-based 'accountability model'. What this means in general terms is that the Regulation should reiterate the principles upon which privacy is to be respected (here we see no need to diverge substantially from the principles of the Data Protection Directive and other international instruments). But rather than prescribing the means for organisations to live up to the principles, the Regulation must identify the outcomes that are expected, give companies the flexibility to create the internal governance that achieves those outcomes, and use certification programmes, third-party audits and judicious oversight and enforcement to ensure that those outcomes are met.

Contents

See Amendment 1 in the attached annex

1. *Set high-level principles and expected outcomes in the Regulation.*

We believe the existing framework of both the Directive and the Regulation achieves this. The principles are there, and they are solid. The expectations have been set for meeting data subjects' rights with respect to access, transparency and control.

4. *Accredit independent assessors and seal programmes that perform the oversight function. Develop incentives for industry to use them and report on their results.*

Regulated organisations should be encouraged to commission accredited independent assessors to review their privacy programmes and provide reports to regulators and to the public on their compliance. Those who commit to independent assessment and transparent reporting should receive a waiver of the Regulation's more prescriptive elements on documentation and prior authorisation – the assessment and reporting would replace these now redundant oversight mechanisms.

See Amendment 5, Article 34

The Regulation must incentivise uptake by making commitment to accountability and an effective internal privacy management programme (as we describe later) a mitigating factor in any sanctions imposed. Of course, organisations that do not, for whatever reason (be it size, maturity of the programme or perceived risk) see the value of an accountability programme should be able to continue under the existing regime.

For instance, the Working Party or EDPB could be empowered to certify independent assessors to conduct assurance monitoring and reporting, and organisations could be encouraged (or even required, in some circumstances) to retain such independent assessors to monitor and report on their compliance with the principles set out in any second-generation framework.

See Amendment 7, Article 39

Because the supervisory authority retains ultimate control over the accreditation of assessors, this framework enables a scaling of the supervisory regime using market forces. Those who can afford to (because the economic gains justify it) will pay an independent assessor so that they can act quickly in the marketplace, spurring rather than impeding technological innovation and shifting the regulatory cost to the market rather than the public purse.

Those who choose not to pursue an independent assessment can of course continue to rely on the supervisory authorities' oversight using the traditional prescriptive mechanism – the existence of an alternative approach should free up resources so that the authorities can act in a timely manner, making this a better approach for all involved.

See Amendment 2, Article 22(3), Amendment 3, Article 28(1)-(2), (4)

***Precedent:** Article 29 Working Party points to financial, competition laws*

Outside of the environmental space, the Article 29 Working Party in its 2010 document on accountability discussed various additional precedents in financial services and competition compliance spaces for the model we discuss here.

"Outside the world of data protection, there are some examples of accountability - as a program specifying a data controller's policies and procedures to ensure compliance with laws and regulations. For example, compliance programs are mandatory under financial services regulations. In other cases, compliance programs are not mandatory but are encouraged, such as in the field of competition law. For example, in Canada, the Competition Commissioner has developed elaborate policies on corporate compliance programs. The decision on whether or not companies apply a program is voluntary. However, the Canadian Competition Commissioner stresses the importance of compliance as a risk mitigation tool and stresses the legal, reputational and economic benefits."[7]

How must organisations comply?

The elements of internal accountability governance have been discussed by many other commentators. We'd like to elaborate here on what we built and the precedents we borrowed from that guided us, as a potential model for the regulatory framework that can encourage other companies to follow.

1. *Culture, not "tick-box" compliance*

The companies who have made the most progress in reorienting their approach to privacy have been those that make privacy a matter of corporate culture rather than just legal "tick-box" compliance. We take as precedent the UK Bribery Act 2010 (see sidebar), which encourages regulated industry to take steps to internalise their commitment to compliance by, for example, setting the tone at the very top of the organisation and creating a sense of ownership and responsibility throughout the organisation (not just with lawyers and compliance experts) through training and communication.[4]

See Amendment 2, Article 22(2)(b)

2. *Operationalising privacy risk management*

Environmental regulations have one aspect that has been widely credited with truly internalising compliance within a company – the Environmental Management System, which applies advanced business management practices to the environmental aspects of a company's operations. It turned companies' internal environmental compliance programmes from

Precedent: Mandatory and voluntary public reporting regimes

Reporting regimes have been mandated successfully in other sectors (for example, their long use in areas of accounting and finance). There is also an extensive practice of voluntary reporting, for example in corporate responsibility through independent assurance standards like AA1000 APS (Principles Standard), launched in 2008, which provide a recognized basis for organisations to report on their compliance with principles.[8]

Although tarnished in this economic environment, the fundamental model for this kind of oversight is clearly the regulation of accounting and the financial services. It can be argued that the failure of this model there was not due to inherent weaknesses in the model itself, but in the failure of the oversight and enforcement role. We believe that the framework discussed here, when combined with the dedicated regulatory bodies of the existing Directive, can prove a powerful combination.

nal evidence of their internal privacy management programmes, and must provide incentives for organisations whose size or risk profiles justify the retention of independent assessors to verify their programmes and publish reports on their overall compliance. One strong incentive would be removing other prescriptive requirements for those organisations that do so. This would be a far more effective mechanism in creating transparency and accountability than the existing requirements. Documentation requirements of the kind we propose will also serve as a solid foundation for the kind of oversight and enforcement we discuss below.

See Amendment 2, Article 22(3)

How will the Regulation be enforced?

Any regulatory model will succeed or fail on the strength of its oversight and enforcement model. Organisations must be held to account for their record in implementing the data protection principles and achieving the outcomes required by the Regulation, by whatever means they have adopted.

Supervision is currently the monopoly of the national regulator, and this creates both a resource and skills bottleneck. It is clear that we need to explore alternatives to direct supervision by regulators. National regulators frequently cite lack of resources as a major impediment to their supervisory role. The increased use of codes of conduct, as we call for above, will place further pressure on the scarce public resources of our regulators.

The solution is to create the independent monitoring and assurance programmes we discussed earlier. In this supervisory model, regulators are required to accredit independent assessors who can be commissioned by companies to review their privacy programmes. Such assessors are then empowered to provide reports to regulators and even to the public.

In a similar vein, 'privacy seals' and trust programmes can provide independent assessment on a more limited basis, such as for specific products or technologies, as illustrated by the good work of organisations like EuroPrise.

See Amendment 7, Article 39

Importantly, this model will stimulate the creation of a secondary market in privacy compliance assessment, reducing the pressure on regulators as a resource bottleneck, but remaining accredited and approved by the regulator. It will lead to the development of a professional community of skilled privacy assessors with the goal of helping enterprises (public and private) develop the internal culture and professional support structures necessary to embed privacy compliance within their organisations.

Independent assessors would also be in a position to gather feedback and learning from the assessment process that can, without compromising the confidentiality of individual companies, act to inform and educate both the regulator and policy makers more generally about what is happening on the ground.

Conclusion

We are strongly pro-regulation. Industry will never improve its privacy track record without clear obligations and strong enforcement. But more prescriptiveness is not the answer. Privacy is too important to be marginalised in the corporate legal department.

Strange though it may sound, the new Regulation must embrace ambiguity – uncertainty in regulation is not necessarily a flaw. Designed into the right framework, it can impel companies to empower strategic professionals to make risk-based, business-oriented decisions that produce better outcomes than prescriptive rules could. And it must be accompanied by strong and effective enforcement, with significant impacts for companies that get it wrong. Policymakers have to be bold to allow ambiguity. But it's not a compromise, it's an essential element of a successful regulatory framework.

[1] Examples of regulatory covenants in six European countries were described in a 2011 report of the European Environment Agency, which states, "By 1996 more than 300 EAs