The Evergreen privacy programme — myth or reality?

Kate Brimsted, Data Privacy and Security Lead at Bryan Cave Leighton Paisner LLP, offers advice on how to build a flexible and timeless privacy programme

Though perhaps falling short of being a universally accepted one, it is a truth that any organisation processing personal data needs a privacy programme. But how best should an internal compliance framework be structured in order to keep apace with the rapid rate of change and remain relevant (if not necessarily interesting)?

As more countries are enacting comprehensive data protection laws for the first time, the question becomes increasingly relevant. Even the US appeared close to passing a Federal data protection law earlier in 2022, whilst other countries (for example, Australia, the UK and Switzerland) are in the process of updating existing legislation and/or introducing complementary legislation. The EU also continues to generate new laws, a good example being the EU's Digital Services and Artificial Intelligence Acts.

So is it realistic for organisations with operations in multiple jurisdictions to attempt to construct global programmes which serve their current requirements consistently, avoid jurisdictional silos and yet allow sufficient flexibility to remain 'vital'? This article discusses some of the features and approaches which organisations may be able to deploy in service of such an aim.

Where to start

The main components of an evergreen programme are likely to be the same as for any organisation-wide privacy programme, with some additional areas of focus.

The UK Information Commissioner's Office's ('ICOs') Accountability Framework ('the Framework') serves as a helpful starting place for potential components. Indeed, the Framework itself explicitly notes that it can be used for a number of purposes, including creating a comprehensive privacy management programme, checking existing practices against the ICO's expectations, considering whether existing practices can be improved, understanding ways to demonstrate compliance, recording, tracking and reporting on progress, or increasing senior management engagement and privacy awareness across an organisation. It identifies eight different areas of compliance programmes (which the table on page 7 distills into six). These are not independent areas and in order to maximise effectiveness, there needs to be a degree of inter-connectivity between them, for example, between governance and risk assessment/ monitoring.

A dynamic approach to internal compliance will likely necessitate a larger budget. As with any compliance programme, there also needs to be a continuous, consistent investment of resources in order for it to remain effective and relevant. Although it is relatively inexpensive to purchase a set of template policies, write privacy policies and adopt standard processing contracts for suppliers, such efforts alone do not make for effective privacy programmes. Given that the support of the senior leadership is key to success, some attention also needs to be given to how to ensure such support.

How to win (management) friends and influence people

Many readers will recall the intense lead up to the GDPR's entry into force on 25th May 2018. The imminent introduction of sanctions and potential fines on such an unprecedented scale provided a large boost to data protection professionals pitching global data privacy compliance programmes to corporate leadership. However, although the sanctions 'stick' was undeniably a good incentive, an alarm-based approach tends to fatigue after a while, with data privacy 'fires' being overshadowed by the next big regulatory inferno.

An antidote to this is for internal privacy teams to position themselves as harbingers of good news rather than doom. To be able to recount a positive story about the virtues of an embedded and functional privacy culture inspires rather than alarms. Such an approach tends to be characteristic of the most successful data privacy functions within organisations, where privacy professionals have forged a 'trusted advisor' role that has helped engender a culture of respect towards personal data usage, as well as the empowerment of colleagues outside of privacy teams.

It is all too easy for data protection to suffer from image problems within organisations, particularly in the private sector. Avoiding being viewed as the internal 'data police', becoming the 'can do' rather than the 'can't do' advisors is helpful on the path towards gaining allies and ultimately being involved in shaping corporate strategy. Further, by making friends at the grass roots levels, data protection teams can acquire advocates from across the organisation (for example, from information security, legal, compliance, product development, HR and marketing teams). Through taking a constructive approach, privacy professionals can aspire to influence and inspire the C-suite in a more sustainable way, and not just at the outset of programmes. Such a constructive approach includes celebrating the wins with the rest of the organisation, resulting in a reduction in customer complaints.

The evergreen paradigm

Like an evergreen tree which stays fresh from season to season, the defining feature of an evergreen privacy programme is its flexibility when it encounters change. A good, resilient programme also takes into account changes in the future direction of the organisation, including new product and service offerings, organic and inorganic growth (for example, acquiring new group companies or businesses) or a changed geographic footprint.

Most organisations will have some form of framework already established. However, established programmes can still be adapted and improved.

Key to the evergreen paradigm is building in ongoing monitoring of the performance of a programme. Often, monitoring is interpreted as meaning incident management, with the possible addition of data subject request response Key Performance Indicators. Although important, these activities fall far short of constituting a meaningful assessment of an organisation's programme. Measuring the performance of the programme means being able to validate its success and vindicate its investment both to date and prospectively. It should also allow a 'course correct' before things diverge too far, for example, if no Data Protection Impact Assessments ('DPIAs') are being carried out. More fundamental questions, for example, whether programmes designed to meet the requirements of the GDPR are still the correct benchmark, may also need to be revisited over time.

Performance monitoring needs to be done in a manner that guards against complacency. Paradoxically, if a programme is going "too well" then the current economic environment may trigger pressure to reduce the resources allocated to privacy compliance. Where an internal privacy programme is concerned, savings should be achieved through increasing efficiencies (for example, digital tools to save employee time on repetitive tasks, supporting the DPIA, Legitimate Interests Assessments ('LIAs') and data subject response processes) and not by reducing the scope of the programme.

The demand for experienced data privacy professionals is well-documented. However, it is not just a question of finding individuals with the correct skillsets; organisations need to find the correct personality fit. Apocryphal accounts abound of conflict between Data Protection Officers ('DPOs') and their organisations due to poor cultural fits or a lack of understanding of the role (on both sides). Privacy teams needs to be attuned to the product development process and help those teams to operationalise privacy by design for the organisation.

It should never be underestimated just how important the communication style and softer skills of the privacy team leadership can be. It's interesting to reflect on the increase in skills diversity in the privacy profession.

An in-house privacy specialist may have a background in IT, risk and compliance, HR, marketing or law to name a few. Like the programme itself, recruitment into the organisation's privacy function should be flexible in order to attract and retain people from non-conventional backgrounds, especially those with good communication skills and a broader perspective.

Pulling it together

The table on page 15 aims to bring together the various pieces and highlight factors important for achieving an evergreen programme.

Even though establishing and running a flexible programme will need more investment than a comparatively static one, the evergreen approach will reap more benefits in the medium and longer term. In fact, such adaptability is likely to save money in the long run, as it avoids the need to replace a programme which has become irrelevant and no longer fit for purpose. By being more relevant, timely and effective, evergreen programmes offer greater protection for the organisation from the most significant risks associated with non-compliance (i.e. fines, litigation and brand/reputation damage).

Fundamentally, achieving an evergreen global privacy programme is not about big budgets, regular steering group meetings, cutting edge digital tools or even partnering with experienced external privacy counsel. It boils down to one thing: the internal privacy function. It is this which determines the success, flexibility and relevance of privacy programmes.

Reading the cultural runes of the internal corporate environment and external sectoral shifts, understanding management strategy and aligning with it where possible (and seeking to shape it where it throws up significant privacy risks), and communicating the value of data privacy with imagination and persistence will all reap benefits.

Kate Brimsted
Bryan Cave Leighton Paisner LLP
Kate.Brimsted@bclplaw.com