How to Benchmark and Strengthen Your Privacy Program

axiom

Introduction

Privacy regulations are proliferating and increasing in complexity. These regulations present a growing operational challenge for companies across the globe, especially those subject to multiple jurisdictions where overlapping obligations are inconsistent.

On a recent webinar, privacy professionals Jo Ann Lengua Davaris, Vice President, Global Privacy, Booking Holdings Inc., and Khizar Sheikh, Axiom Privacy and Cybersecurity Lawyer, shared actionable advice about what works and what doesn't to benchmark and strengthen your privacy framework. The webinar was hosted by Axiom and the International Association of Privacy Professionals. Below is a summary of actionable takeaways from their discussion that legal leaders can use when building and maintaining a privacy program and responding to evolving regulations. These include the impact of the Schrems II decision/invalidation of Privacy Shield.

Jo Ann Lengua Davaris
Vice President, Global Privacy
Booking Holdings Inc.

Khizar Sheikh
Privacy and Cybersecurity Lawyer
Axiom

CLICK HERE FOR THE AUDIO RECORDING

Best privacy practices and common pitfalls to avoid

DO

✓ Prioritize a phased approach to building a program

- Build a team of privacy professionals, partners, ambassadors and allies
- Support a culture of privacy that seeps into the core of every employee
- Create a privacy framework, including governance model, set of standards, principles, guardrails, and clear roles and responsibilities

✓ Create an adaptable privacy program to keep up with changing regulations

- Define guiding principles, non-starters, and ground rules
- Focus on the right Key Performance Indicators (KPIs)
    1. *Do you have policies and governance model?*
    2. *Do you do what you say you do in your privacy program?*
    3. *Is privacy by design up and running?*
    4. *Do you have a strong incidence response and metrics?*
    5. *Are you conducting training and awareness?*
- Monitor, test, and evolve your program as needed

✓ Implement ongoing training

- Set up regular communications and awareness modules for specific roles across the company
- Embed privacy into your company culture: use multichannel multimedia to continue training across the organization

DON'T

✗ Treat privacy as a one-off or check-the-box exercise

- Avoid building a program focused on a specific regulation or enforcement action – meeting internal audit standards is not enough
- Walk away from your privacy program once you have built your privacy program
- Assume that a single training is sufficient

How to respond to the Schrems II / Privacy Shield decision

On July 16, 2020, the European Union Court of Justice invalidated the EU-US Privacy Shield Program while upholding the validity of Standard Contractual Clauses.

What companies must do now

- Stop transfers based on Privacy Shield
- Conduct risk assessment for data transfers utilizing another transfer mechanism
- Adopt changes including an adequate transfer mechanism, supplementary measures, or even a data localization option

Key details on the Schrems II ruling

- Despite invalidating Privacy Shield, the Court of Justice agreed that data flows from the EU to the US should not be interrupted
- Standard Contractual Clauses, BCRs, and other transfer mechanisms permitted by GDPR remain valid
- The European Data Protection Board released an FAQ but provided no new practical solutions
- Increased due diligence on the part of data exporters is expected to ensure the privacy laws of importing countries are adequate:
    1. *This may involve a written transfer adequacy assessment that assesses appropriate safeguards in the importing country, taking into account the circumstances of the transfers and supplementary measures.*
    2. *It could include a consideration of privacy laws, security laws, the level of access/surveillance, data subject rights, adequate consent, onward transfer by subprocessors, and appropriate contractual provisions*
    3. *It is not clear what supplementary measures could be appropriate, but the EDPB has indicated that they are working on further guidance*
- If the transfer adequacy assessment concludes that appropriate safeguards cannot be ensured when transferring the data, companies must suspend or end the transfers, or notify their competent supervisory authority

Detail for those relying on Standard Contractual Clauses

- Implementing SCCs will no longer be sufficient
- Both parties will have to take into account:
    1. *The content of the SCCs*
    2. *The specific circumstances of the transfer*
    3. *The legal regime applicable in the importer's country*
- If the parties conclude that the data importer's country does not provide a substantially equivalent level of protection for the data exporter's data, the exporter may have to consider putting additional measures to those included in the SCCs
- Companies must conduct individualized assessments and document those assessments on a case-by-case basis

Align privacy procedures to new jurisdictions

Have a comprehensive governance framework

- Focus on a single set of principles, standards, and processes – note where specific local guidance may have to come into play
- Consider implementing local teams in higher-risk jurisdictions
- Identify the role of the corporate team – do they enforce consistency or approve changes to the framework?
- If the revenue centers and products are local, determine whether the local team is empowered to make changes

Consider your risk appetite

- Understand if your organization has a zero risk tolerance or is more comfortable with risk
- Identify and focus on the common core set of principles between differing regulations
- Prioritize high-risk jurisdictions where you do business and process personal data

How to achieve harmony across your organization

Partner with information security and technology

- Your privacy program is only as strong as the information security program controls built to sustain it
- Harmonize different teams' roadmaps and discuss the risks based on when milestones and commitments can be achieved
- Be upfront with your executive and board members about the risks, what is needed to mitigate them, and what resources and headcount you need to reach key privacy milestones

Recognize there is more to a successful privacy program than legal and information security

- Stakeholders that own data governance functions and/or risk, such as marketing and compliance, may also have to be at the table
- Optimize your legal team based on your risk tolerance – providing advice on the complex area of privacy will be increasingly challenging for generalist attorneys
- Consider adding a legal SME to help design and execute your program

Key actions you can take right now

START WITH THE DATA

Assess your relevant data transfers and find an alternative method if needed

UNDERSTAND YOUR RISK APPETITE

Examine the technical measures that can help you mitigate risk and determine how to build these into your privacy program and principles

BUILD YOUR GOVERNANCE MODEL

- Develop an understanding of local law regarding government access to EU personal data and memorialize these findings
- Develop KPIs that have strong incidence response and metrics
- Embrace a culture of privacy by developing ongoing, comprehensive, role-specific training programs

Whether your company needs help building a privacy program, supporting ongoing privacy operations, or navigating changing regulations, Axiom's bench of 200+ privacy lawyers can provide your team with the experience and expertise that you need.

Get in touch with us today:

axiom@axiomlaw.com

+1 (917) 237-2900

www.axiomlaw.com/contact-us