Forrester's 2016 Interactive Data Privacy Heat Map

Landscape: The Data Security And Privacy Playbook

by Chris Sherman, Enza Iannopollo, Heidi Shey, and Alexander Spiliotes

October 31, 2016

Why Read This Report

To help security and risk professionals navigate the complex landscape of privacy laws around the world, Forrester created a data privacy heat map that highlights the data protection guidelines and practices for 54 different countries. It also covers other relevant issues like government surveillance, cross-border data transfers, and regulatory enforcement. Due to the dynamic nature of data protection legislation, we update information within the interactive tool annually.

Key Takeaways

The EU Adopted The GDPR; Global Preparations Commence

The EU's adoption of the General Data Protection Regulation (GDPR) on April 27, 2016 forces foreign governments and corporations to start preparing for compliance. With barely more than two years between adoption and enforcement, firms around the world that do business with European customers — and those doing business in countries following the GDPR's lead — must now thoroughly examine their privacy and security practices and remediate any control gaps as soon as possible.

Several Governments Push For Surveillance-Enabling Legislation

While some countries increased regulation of corporate treatment of citizen data from 2015 to 2016, several others drafted or passed legislation that could grant governments more access to citizen data. Many countries — and not just ones with histories of surveillance — still struggle to reconcile pressure from citizens to restrict surveillance with pressure to glean national security intelligence from civilian data.

Forrester's 2016 Interactive Data Privacy Heat Map

Landscape: The Data Security And Privacy Playbook

by Chris Sherman, Enza Iannopollo, Heidi Shey, and Alexander Spiliotes
with Christopher McClean, Merritt Maxim, Jeff Pollard, Trevor Lyness, and Peggy Dostie

October 31, 2016

Use The Data Privacy Heat Map To Understand Global Privacy Laws

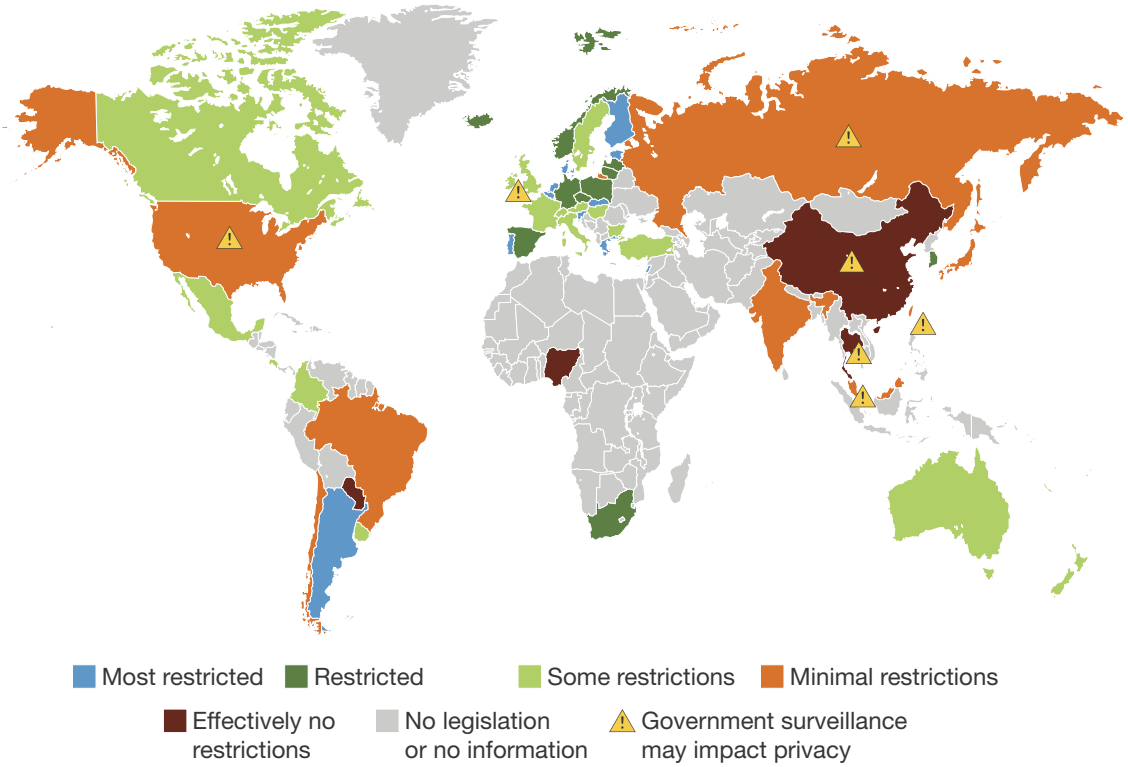
Privacy regulations vary from country to country and often conflict with each other. For a global organization, navigating the patchwork of privacy regulations in countries around the world to develop appropriate privacy policies can be daunting. To help security and risk professionals tackle this challenge for their organization, Forrester created a data privacy heat map (see Figure 1). Click on any of the 54 shaded countries within the map to learn more about country-specific data protection and privacy regulations. Dive deep into the ratings by clicking on "More Info" within the country descriptions, or compare a particular category of requirement country-by-country by clicking on the drop-down "View by" menu and selecting any of the categories of interest. Finally, create handouts that compare multiple countries by clicking "PDF" and selecting the countries most important to your organization.

Begin using the data privacy heat map now. The link will take you to a user authentication page where you will enter your Forrester user name and password to access the interactive tool.

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

FIGURE 1 Landing Page View In The Interactive Data Privacy Heat Map



Ratings Are Based On The Most Relevant Data Privacy Legislation

This interactive map provides information on national data protection laws that either have been enacted or are currently under consideration around the world. It does not address sectoral laws, local laws, or criminal/civil code provisions that may address data protection. It is intended for information only and should not be treated as an authoritative interpretation of the actual laws in these countries, and it may not reflect all recent changes and legislative updates. The data that informs the ratings in the interactive graphic is provided in the associated "2016 Regulatory Landscape" tool (see Figure 2).

We chose each of the seven privacy and data protection categories and associated rating scales based on their relevance to organizations that store and process data in the associated country:

- **Scope of protection.** This category specifies what personal data each country's data privacy legislation protects.
- **Covered entities.** This category specifies the legal obligations placed on public and private organizations in each country.

- **Data transfer to other countries.** This category covers legislation restricting data transfers into countries with inadequate data protection regulation, using the EU's strict regulations in this area as a benchmark.
- **EU adequacy.** The EU has deemed some external countries safe destinations for EU citizen data, based on those external countries' data protection laws. This category shows each country's attainment of the EU's official adequacy standard for data protection and privacy.
- **Data protection agency established.** This category rates each country's ability to enforce data privacy regulations through an agency solely dedicated to data protection and independent of other government.
- **Government surveillance.** Many organizations are deeply concerned about government surveillance, as proof or suspicion of surveillance can have negative effects on business operations and ultimately profitability.[1] This category rates the legislative and cultural barriers limiting government surveillance of communications within each country.
- **Privacy rights established in constitution.** Countries with constitutional backing for privacy are much more likely to regulate and enforce organizations' proper use of personal data. This category specifies each country's establishment of privacy rights in their constitution.

FIGURE 2 2016 Regulatory Landscape

Access the heat map data in the associated "2016 Regulatory Landscape" tool.

How can I access the raw data that informs the heat map?

The data that informs the heat map is available in the "2016 Regulatory Landscape" file that appears on the right-hand pane of the report on Forrester.com. Data displayed within the web tool is detailed in the "Global Summary" worksheet. This information provides a list of countries highlighted in the heat map and contains details about the privacy standards and regulations, as well as a detailed country description, for each country. The "Ratings Key" sheet defines the classification scales on which all 54 countries are measured.

We Evaluated 54 Countries, Each With A Unique Approach To Data Privacy

Our team of security and risk analysts evaluated the privacy laws, practices, and regulatory enforcement of 54 countries. We rated each country in seven categories; the rating scale explanations are found within the interactive tool and associated model. A combination of each country's category-specific ratings make up each country's overall rating (displayed in the "Privacy and Data Protection by Country" rating), ranging from "Most restricted" to "Effectively no restrictions."

Countries such as China and Paraguay, which lack many of the foundational regulations found in most other countries, are examples of countries with "Effectively no regulations." On the other end of the spectrum are those "Most restricted" EU countries with a deep commitment to protecting individuals' right to data privacy, ensuring that governments and private entities alike do not abuse personal data. Between these two groups lies a highly disparate set of approaches taken by governments toward data privacy protection, although a few key trends persist:

- **The GDPR has already begun to raise the legislative tide within the EU and abroad.** The General Data Protection Regulation (GDPR) is the most significant recent data privacy legislation to affect businesses across the globe.[2] The regulation imposes a higher standard of personal data protection, with significant penalties for noncompliance for companies across the European Union (EU). It also applies to foreign companies that offer services or products to EU residents or collect their data. While the regulation is yet to be enforced, it has already had an effect outside of the EU. For example, in March 2016, South Korea enacted stiff penalties for data privacy violations by telecommunications and online service providers in a fashion similar to the upcoming GDPR (up to 3% of total global revenue in South Korea, 4% for the GDPR).
- **Countries continue moving toward the EU standard for data protection.** New legislation outside of the EU often follows the EU's lead by adopting provisions similar to those in the existing Directive 95/46/EC regulation. The slow global convergence toward the requirements outlined in the regulation continued through 2016. For example, Argentina and Japan strengthened preexisting policies, while Nigeria passed its first comprehensive cybercrime legislation. Japan also established an independent regulatory body ("Privacy Protection Commission") that oversees privacy issues — a requirement of both the current Directive and the superseding European GDPR.
- **Attempts to strengthen surveillance undermine data protection laws.** While some countries are reluctant to expose their citizens' data in any way, many others seek more access. For example, Finland is drafting legislation that would give its military and domestic security forces broad access to civilian web communications to gather intelligence. Even countries with a strong and long-standing privacy protection footprint, like Germany and the Netherlands, passed or are about to pass regulations that considerably increase government's surveillance powers. Meanwhile, criticism prompted India to withdraw a law in late 2015 that would have forced companies to store all encrypted electronic communication in plaintext for 90 days. The balance between security intelligence and personal privacy continues to pit governments against citizens.

Recommendations

Define Your Own High-Water Mark For Data Protection

Each of the seven categories of data privacy we used to evaluate countries in this report may present an obstacle for an organization hoping to do business there. As a security and risk professional, you should be aware of the restrictions is each jurisdiction so you can help plan business and privacy practices accordingly.

Use the interactive tool's PDF creation feature to guide dialogue between key stakeholders about the challenges posed by data privacy regulation, then build a high-water mark data protection policy based on the most restrictive countries in which your organization serves customers.[3] This will ideally pave the way toward more streamlined and consistent data protection policy enforcement across your entire organization.

Read The Research

Interested in how data privacy regulations affect security and risk? Read Forrester's research on the significance of data privacy regulations around the world.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iPhone® and iPad®
Stay ahead of your competition no matter where you are.

Endnotes

[1] Since Edward Snowden revealed the US National Security Agency's PRISM spying program, there has been widespread speculation that the announcement would ruin the fates of US cloud, hosting, and outsourcing businesses as international customers walked away from any firm within the agency's reach. In this first survey of these customers about the effects of PRISM, the data suggests such concerns were overblown. And in fact, our earlier contention that enterprises would stick with their US partners but take a stronger position in managing their own security has been proven out. See the "Did PRISM Cause An Exodus From US Clouds?" Forrester report.

[2] More information is available in the upcoming "Brief: Your Action Plan For GDPR" Forrester report.

[3] Data defense is the fundamental purpose of information security. To defend your data, there are only four levers you can pull: controlling access, inspecting data usage patterns for abuse, disposing of data when the organization no longer needs it, or killing data to devalue it in the event that it is stolen. Policy addresses when and how much to pull the levers. Too often, organizations create data policies without a clear understanding of feasibility and purpose within their business because they themselves are in the dark about their data, from what data they have to where it resides. As a result, many data security policies are ineffective and can even hinder business processes. Data classification via traditional frameworks such as Bell-LaPadula and Biba can be too academic in nature and not enforceable in the modern world of big data and advanced threats. In today's evolving data economy, data identity is the missing link that security and risk (S&R) leaders must define in order to create actionable data security and control policy. See the "Know Your Data To Create Actionable Policy" Forrester report.

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.