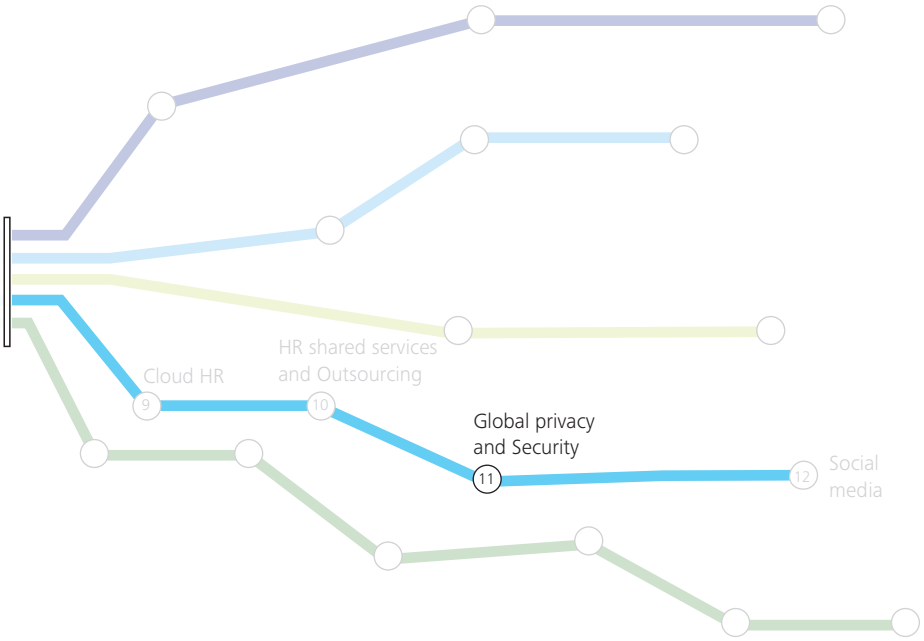
Enabling HR service delivery

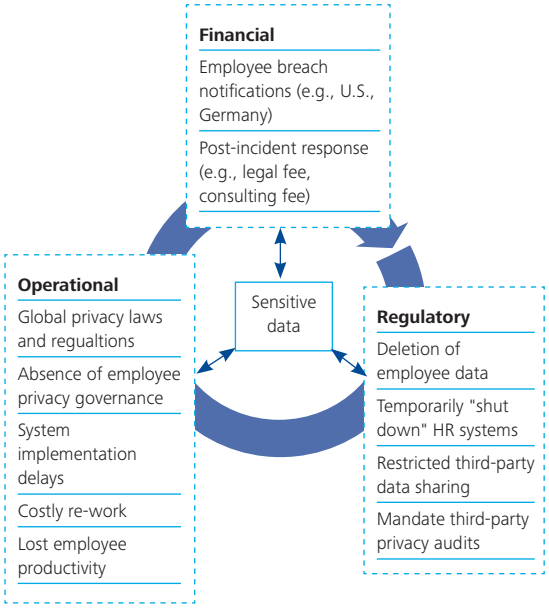


11 Global privacy and Security

The temperature is rising. Protecting your employee data and your organization's information is a topic of discussion not only in your boardroom, but also in courtrooms, union and works council meetings, department functions, and in people's homes. As breaches increase, national regulators and national works councils are taking notice of privacy and data protection weaknesses. They are imposing penalties that range from fines and consent decree mandates to work stoppage or a combination of all three. These penalties are increasing as international regulations continue to grow in number and complexity.

But in HR information security, the biggest risk is failing to meet the expectations of your workforce. Employees are more sophisticated, and they expect their employers to protect personal information and abide by the regulations enacted to protect their privacy.

On the other hand, businesses are still required to deliver a wide range of efficient services, even as they push toward rapid global expansion. Self-service and HR analytics are only the beginning of a list of capabilities your HR service delivery model is expected to possess. Almost all these services increase access to personal information, force HR processes deeper into the organization, and create a more complex environment for protecting data and keeping personal information confidential.



Source: Deloitte

Solutions arise from challenges — and vice versa

The technology solutions and service delivery models behind these changes provide new utility, but also offer new risks. SaaS applications, cloud computing, smart phones and mobile applications, and social media and HR analytic applications lie at the cornerstone of many transformation efforts. These technologies change the landscape of privacy, including the ways in which data is protected, how regulators assess their use, and how employees perceive the security of their personal information. Outsourcing and insourcing various functions of service delivery also create new challenges. Many organizations struggle to understand how privacy, data protection, and risk relate to one another. When contracting and monitoring third parties, or when assuming activities in-house, it can be difficult to know how to address privacy and data protection controls in areas, such as cross-border data transfer mechanisms, notice, choice, and information confidentiality.

As in any transformation effort, leaders are faced with managing conflicting objectives. Under pressure to provide more services across a broader, international geography, how can you do it with the privacy and data protection controls your employees demand?

Before tools, understanding

The solution resides in understanding the components of privacy and security and how data flows to, through, and from your organization. "Privacy" relates to personally identifiable information (PII) and the ways an organization works to use and disclose it properly. Within the context of HR, privacy is how you manage the rights and obligations related to personal data within your workforce. "Security" is more general — it describes the way an organization protects information and systems from unauthorized access and use. The trick in HR Transformation delivery is to integrate both privacy and security throughout your HR services and the systems that support them.

Global privacy strategies are often driven by the cross-border transfer mechanisms an organization selects and is a way it positions itself to meet the requirements of these mechanisms — for example, notice, choice, access, or onward transfer. To meet privacy requirements and build a sustainable model for HR service delivery, organizations must incorporate these requirements into either new or existing components of governance. The decisions to be made include ones focused on policy, procedures, roles and responsibilities, training and communication, monitoring, and controls.

These requirements can differ from country to country, so companies should evaluate them through the lens of risk — using a consistent approach that addresses key regulatory requirements that are common across many international regulations, while still supporting the local management of relevant outlying requirements. In this process, companies should assess the risk associated with regulatory compliance in the countries where they do business. They should also consider specific privacy and data protection risks in the way personal data is captured, used, transferred, stored, and destroyed — whether it happens within processes, within systems, at third-party vendors, or within the various formats and views through which personal data will "live" within your organization. The transformation program should include a careful approach to evaluating these specific risks and to embedding control designs within the data flow of your organization.

Security is a component of privacy, and it relates to data protection measures, such as access controls and data encryption. But it also encompasses a range of capabilities found within HR Transformation, including identity management, application security, and business continuity. It is important to build transformational solutions that are designed to secure data from internal and external intrusion. Security is addressed at the enterprise level, with services and solutions designed to integrate with the ways a company manages its overall business, not just HR.

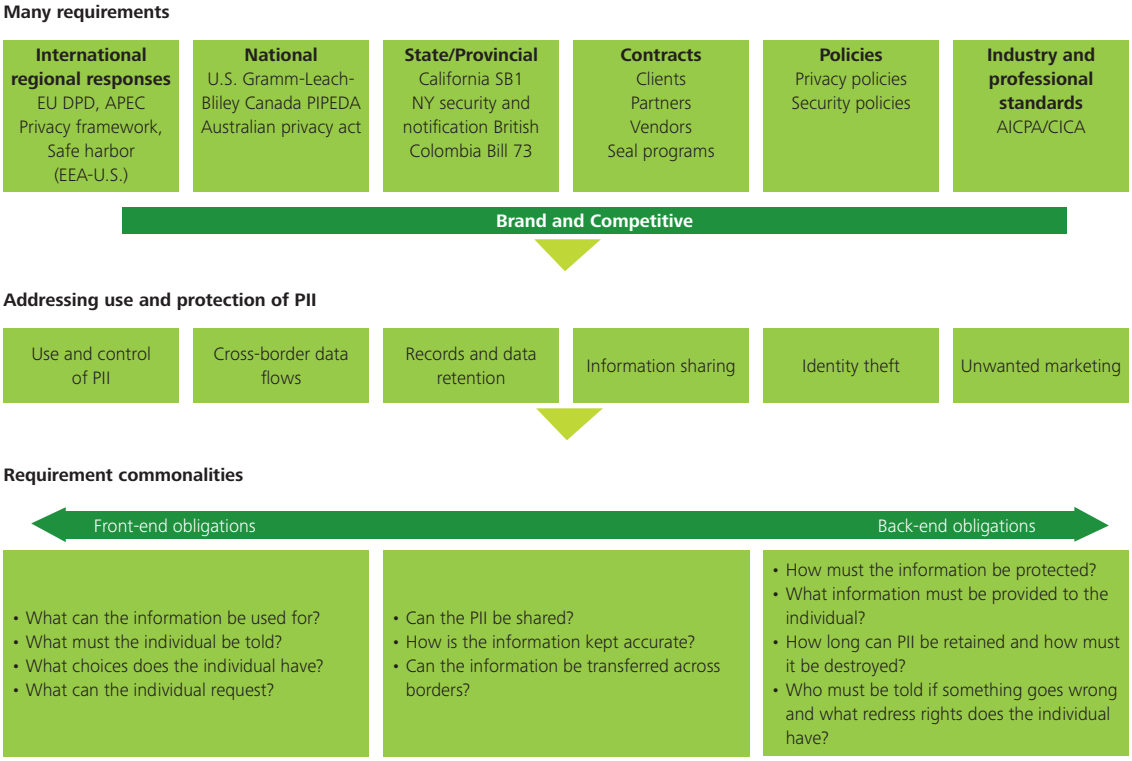
Case study

As a global manufacturing company embarked on a journey to consolidate numerous and disparate HR systems, its management realized that there was a significant risk to the project if privacy and security were not considered from day one. To help mitigate this risk, management added a privacy team to the project that focused on dealing with these specific requirements for the consolidation.

The team first tackled the problem of identification of global requirements associated with international laws, standards, and works council requirements. The privacy team was helped by a knowledgeable legal support team, global management with a grasp of existing requirements, and IT security team members.

Next, in order to understand how these requirements affected the future state business processes associated with the consolidated HR system, the "to-be" processes were mapped and controls were designed accordingly. Requirements and controls were also developed for the broader security components, including application security and the integration of the new HR system with their global identity management system.

Finally, specific privacy and security governance components, such as an organizational structure, policies and procedures, and a cross-border data transfer mechanism strategy were designed and put into place. The work helped define a more overall approach to privacy and security for HR and led to the establishment of a Global Employee Privacy Program for the organization.



Source: Deloitte

It is a mistake to integrate these "IT" security solutions and controls as an afterthought in an HR Transformation. A true transformation requires the planned integration of security strategies, capabilities, and resources. This needs to be part of the larger HR Transformation and its related privacy programs. Global roles, seamless application access, application controls over how systems can be used, business continuity options, and plans are designed better and provide more value when leaders manage them holistically with the broader transformation.

Factors to a holistic approach

In building a holistic approach to meeting privacy and security requirements within HR Transformation, an organization can deliver sustainable ways to comply with global regulations and define efficient methods to protect data. Key factors to a holistic approach include:

Cross-functional executive support. Privacy and security is a cross-functional issue that requires strong executive support and involvement across areas, such as business, IT, HR, and legal.

Data lifecycle. Before you can understand how to implement reasonable controls, you first need to understand where the sensitive data is and how it is used, from collection through destruction.

Risk-based approach. Focusing on business risk (as opposed to merely compliance) and identifying and prioritizing high-risk items can increase the value the privacy and security solutions can deliver.

Change management. The usefulness of the privacy and security solutions come down to what people do on a day-to-day basis, so preparing, educating, and holding accountable appropriate professionals is vital.

Implementation focus. Because most serious problems occur when policies do not match operational practices and capabilities, it is critical to go beyond policy development to actually operationalizing the policies in business processes and technology.

The holistic approach offers a practical solution to one of the biggest challenges of privacy. It can quickly assess the risks of global regulation, allowing companies to focus privacy and data protection efforts on the activities that address the real regulatory issues related to cross-border data transfer, onward transfer, and secondary use of PII.

Ready to grow

As organizations prepare to compete for high quality talent globally, they need to redefine what privacy and security means. They are not just about compliance. Together, privacy and security constitute a valued asset to an organization and its workforce. Achieving this takes an understanding of the privacy and security solution and each of its components. It is important to make delivery of privacy and security a part of the transformation strategy — to integrate it in planning, design, and delivery. The right specialists and tools can help the plan avoid confusing technical solutions and navigate the maze of global laws and requirements.

Organizations that plan, embed, and deliver privacy and security within HR Transformation — as a sustainable part of the new structure — do not feel heat from either regulators or employees. On the contrary, they see real strategic benefits. They are able to exploit new technologies safely. They can deliver efficiently and avoid costly "refitting" of security and controls after the transformations. And they can have more agile organizations that can expand into new global markets without the worry of unprotected systems and information.