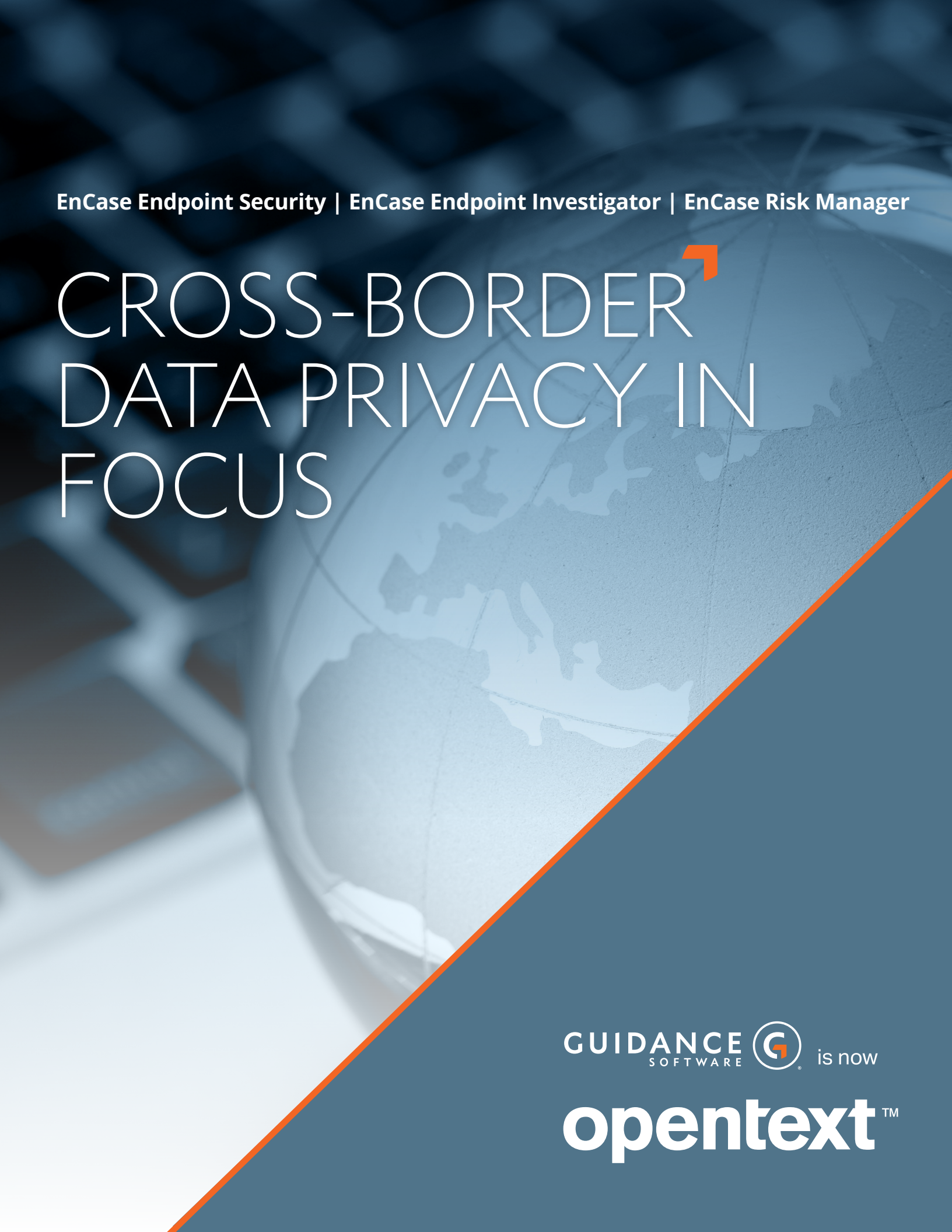


EnCase Endpoint Security | EnCase Endpoint Investigator | EnCase Risk Manager

CROSS-BORDER DATA PRIVACY IN FOCUS

GUIDANCE SOFTWARE is now

opentext™

OVERVIEW

Organizations continue to grow globally, not only in market reach due to an increasingly connected world, but by office locations, employee distribution, and operational extension. For mid-sized businesses in the U.S., 66% of decisions makers said they have tapped international markets as a way to acquire new customers, 55% said they are reaching out to find new suppliers for products and services, and 46% said they are manufacturing products internationally[1]. For global entities, the amount of data that is produced, processed, and transmitted across borders has also grown exponentially. Cross-border data flows have increased 45 times larger since 2005, and are projected to grow by another nine times by 2020[2]. Whether or not this cross-border data contains customer information or financial records, the need to proactively identify and manage private and sensitive information is paramount. This is true especially in light of increasingly complex regulatory mandates like the E.U. General Data Protection Regulation (GDPR) and the Privacy Shield.

Cross-border data transfer issues will likely remain a top priority, particularly for the EU. Organizations should start the process of designing and implementing a privacy-compliant cross-border data transfer strategy now, as this can potentially become a very lengthy and drawn-out process. In this paper, we will review several cross-border data privacy regulations, the data-related challenges facing organizations today, and how Forensic Security products from Guidance Software – EnCase Endpoint Security, EnCase Endpoint Investigator, and EnCase Risk Manager - are well positioned to provide solutions that addresses these problems.

---

[1] "How Smart Companies Are Expanding Globally." American Express Global Corporate Payments. August 2016.

[2] "Digital globalization: The new era of global flows." McKinsey Global Institute. February 2016

CHALLENGES TO CROSS-BORDER DATA PRIVACY

With the increasingly complex and constantly changing regulatory landscape, there are many important questions to ask about cross-border data privacy. Questions like, what invokes cross-border data transfer issues? What types of safeguards will ensure an adequate level of data protection? Are there requirements to demonstrate how sensitive information in one country is handled by data administrators in another? Answering these questions, among others, will require careful and strategic combinations of both data governance policies and enterprise-level data management technologies.

First, it is important to gain a firm understanding of any organizations' sensitive data landscape, particularly how this data manifests throughout the business. Basic questions need to be answered – like, what is considered sensitive data and where is it located across the organization? And is any of our data under export controls? It is important to note that sensitive data may look different for each organization. For instance, retail firms may be most concerned about customers' financial data while pharmaceutical companies may prioritize the protection of intellectual property and proprietary trade secrets. There is also a need to "define" sensitive or private data, determine whether it is critical or of no business value to the organization, and then identify where that information resides by country.

Another primary challenge stems from the complexity of global data privacy regulations that vary from one country to another. In Europe, the transfer of personal data from within the EU to countries outside the European Economic Area (EEA)[3] is prohibited unless adequate levels of privacy controls are assured. There are exceptions to this rule, but the fundamental principle is that EU countries currently restrict data transfer to countries outside of the EU. However, it is equally important to closely examine each individual country's data transfer requirements as some EU countries have higher standards for data privacy than others. While the GDPR establishes minimum levels of protection and uniformity, any country can voluntarily implement more stringent data privacy mandates. And to make matters more complicated, the transfer of data to/from former EU countries, like the U.K.[4], may trigger other data privacy related complexities. Speaking broadly, the challenge is to systematically collect, cull, and review data in-country under local rules unless specific derogations exist.

Lastly, with regulations constantly changing, companies need to revisit internal data governance policies and operational workflows, reevaluate existing agreements with third parties, and determine levels of compliance with Data Protection authorities. For example, organizations should carefully examine their data retention policies to understand the business purpose for each type of sensitive information and then institute a defensible disposition program to ensure data is not retained longer than necessary. Possessing sensitive information longer than required for its intended business purpose can place organizations at risk for data loss or theft, regulatory non-compliance, and electronic discovery of potentially damaging information. Unfortunately organizations are often unable to effectively delete data due to a lack of insight into the information environment, a breakdown in corporate governance, and fear[5]. In addition to the challenges related to data retention policies, all third-party data transfer agreements should be regularly reexamined, and any outstanding concerns with Data Protection Authorities, or other regulatory bodies, should be addressed.

[3] A file located in the EU that is "viewed" from the U.S. or any foreign country is considered a transfer of that data

[4] "Will Brexit Undermine U.K. Participation in the General Data Protection Regulation and the U.S./E.U. Privacy Shield?"

[5] "Quantified Information Governance, A New Path to Value from Data." Information Governance Initiative. March 2016

THE GUIDANCE SOFTWARE FORENSIC SECURITY SUITE

Guidance Software offers a suite of best of breed forensic security solutions to help organizations manage, protect, and investigate their most critical business data. The forensic security suite includes EnCase Risk Manager, EnCase Endpoint Security and EnCase Endpoint Investigator.

First, EnCase Risk Manager helps organizations identify, categorize, and remediate sensitive information across the enterprise, whether that information exists in the form of personally identifiable customer data, financial records, or export-controlled intellectual property. And while the ability to search for standard patterns like national identification numbers and credit card data is straightforward, its true power lies with the ability to discover entirely unique or proprietary information specific to a business or industry. Risk Manager is able to identify this information throughout the enterprise wherever unstructured data is stored, be it endpoints, servers, cloud repositories, SharePoint, or Exchange.

EnCase Endpoint Security can then help to plan, implement, or optimize any organizations' security strategy with the ability to expose unique risks, target gaps in endpoint visibility, and detect threats which have gone unseen by perimeter solutions. The effectiveness of Endpoint Security lies with its ability to accelerate the detection of malicious activity and remediate it before it causes irreparable damage or data loss. So while EnCase Risk Manager is designed to proactively reduce the surface area of digital risk, EnCase Endpoint Security is designed to quickly detect and respond to security threats.

Lastly, EnCase Endpoint Investigator has the power to comprehensively analyze and uncover the root cause of any data breach, whether the threat was internal or external. With EnCase Endpoint Investigator, security teams can perform remote, private, and secure internal investigations of sensitive data loss or theft with no disruption to business operations or employee productivity.

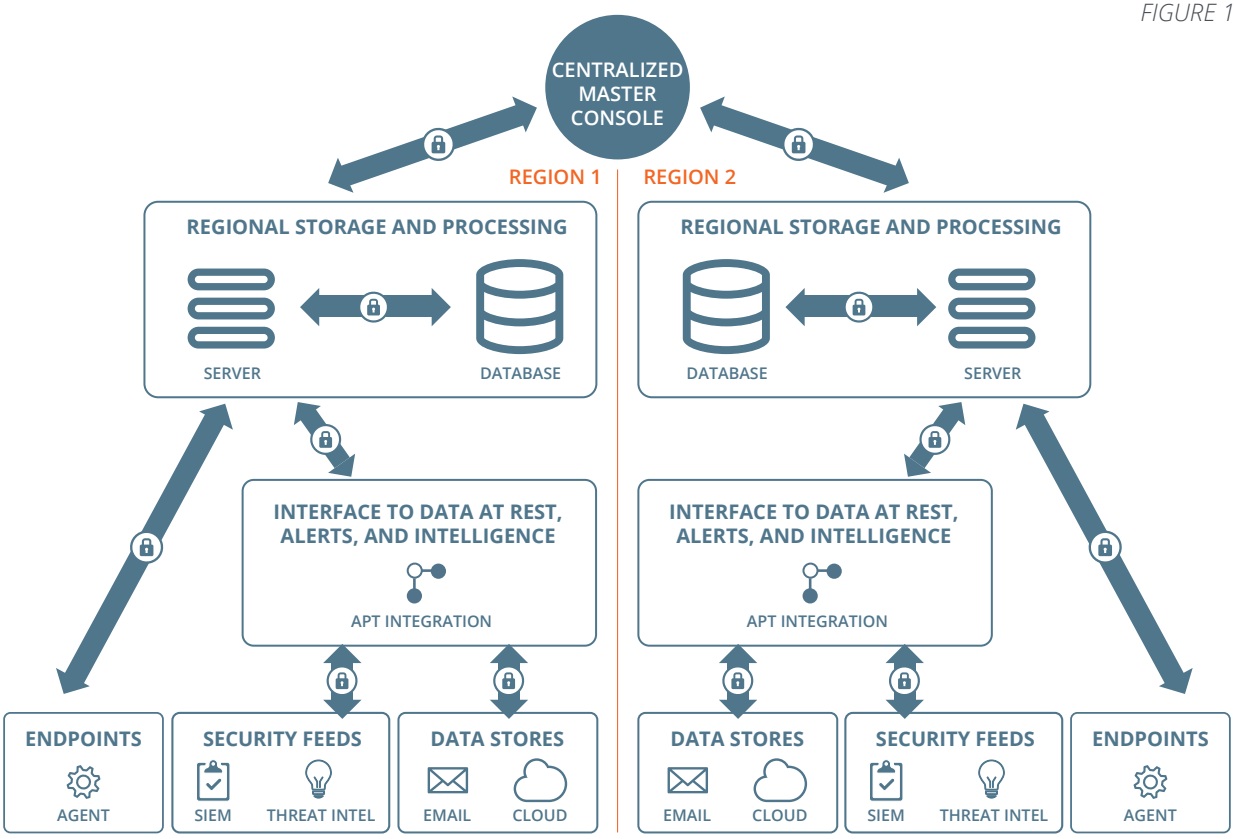
ENCASE: DESIGNED TO MEET THE NEEDS OF GLOBAL ORGANIZATIONS

As it relates to cross-border deployments, the three most significant advantages of the EnCase Forensic Security suite are the flexible platform deployment model, security-by-design framework, and single unified and trusted agent architecture.

STEP 1: FLEXIBLE DEPLOYMENT

EnCase solutions can be deployed within centralized in-country regions to meet data privacy requirements. For instance, site servers and examiners can be installed in-country to ensure all data is processed and stored locally or to a UNC path in the region, which is configurable by the owner. Once the data is stored locally, remote viewing and analysis of segregated data can be conducted in-country as well. For multinational organizations with footprints in two or more countries, a centralized console with data-minimization features can be deployed to report on aggregate sensitive data without transferring any files across borders (See Figure 1). This enables organizations to prioritize by country, create baseline reporting, and demonstrate regulatory compliance. It is important to note that some competitors to EnCase Endpoint Security rely on peer-to-peer networking which completely neglects in-country data segregation and integrity, or are unable to contain what data moves across their systems.

FIGURE 1



STEP 2: SECURITY BY DESIGN

Guidance Software provides market-leading forensic security applications to FTSE and Fortune 100 companies and hundreds of government agencies worldwide. Accordingly, deep forensic capabilities and advanced security features are inherently built into each of our solutions by design. Whether searching for private or sensitive data that may be encrypted, deleted, hidden, locked, or otherwise hard to find, or ensuring that any visibility into the disk is strictly controlled using Public Key Infrastructure (PKI) handshakes, users are able to maintain a high degree of confidence that their country-specific data is not seen by unauthorized parties.

EnCase products also utilize targeted search technologies to scan enterprise endpoints prior to collections to ensure only relevant files are collected and processed; and once collected, they can only be reviewed and accessed by administrators. If the decision is made to delete select files, similar to an infected file, it can never be retrieved or restored by unauthorized parties.

STEP 3: SINGLE UNIFIED & TRUSTED AGENT

EnCase products utilize a single unified agent that is trusted internationally with over 33 million deployed globally. This agent, which is universal across all our security solutions, allows for an efficient eco-system of proactive sensitive data management, endpoint detection and response, and investigations. Time-tested and court-approved with the highest levels of security and reliability, the unified agent sits at the kernel-level and has complete forensic access to all users, systems, and communications.

When agents are deployed, they are keyed to a specific server within a given geographic location. If users travel outside that region or country, any other server will be unable to scan, collect, process, or review files on that particular endpoint running that agent. Therefore, the physical location of endpoints will not violate cross-border data privacy restrictions. If sensitive data is suspected to have transferred, manually, from one in-country network to another, the target network can be subsequently scanned to identify that information. Again, only the agents tied to an in-country server will be scanned, ensuring compliance with data privacy regulations.

.

INCREASINGLY COMPLEX REGULATORY LANDSCAPE

Designing and implementing a privacy-compliant cross-border strategy for data transfer is a complex and challenging task. It requires an understanding of the multinational data landscape and the applicable legal requirements that vary between countries. Moreover, a full risk analysis on data transfer vulnerabilities and the adequacy of data protection must be evaluated and executed to determine what additional safeguards, if any, should be instituted. This adds a level of complexity to the already daunting task of understanding how your organization processes, controls, or maintains personal data across borders and the regulations that govern them. Some of the cross-border data privacy regulations and related market trends that should be considered are described below.



EUROPEAN UNION (EU)

General Data Protection Regulation (GDPR)

On April 27, 2016, the E.U. GDPR replaced the Data Protection Directive 95/46/ED (codified in 1995) and will go into effect on May 25, 2018. The new GDPR is intended to strengthen the data protection rights of individuals within the EU (e.g., data portability, right to be forgotten, profiling, etc.) and unify cross-border data rules for organizations with footprints in more than one country. In addition to the focus placed on expanding or enhancing the rights of EU citizens, the GDPR also imposes compliance obligations directly on data processors. These responsibilities can range from applying security standards, notifying the data controller of data breaches, appointing a Data Privacy Officer (if applicable), and maintaining records of processing activities, among others. Data Processors will be directly liable in case of non-compliance and may be subject to direct enforcement action. It is important to note that the GDPR is not a directive, but a regulation. Non-compliance can also result in fines up to €20M or 4% of annual global revenue.

Whether or not cross-border data contains customer information or financial records, the need to proactively identify and manage private and sensitive information is paramount.

5 GDPR RULES TO CONSIDER:

1. **Extent of Reach:** The GDPR not only applies to data controllers and processors in the EU, but to those outside the EU where their processing of personal data relates to the offering of goods or services to data subjects within the EU - this applies to free goods and services and the monitoring of behavior.
2. **Data Records:** Data controllers and processors must maintain accurate records of all data processing activities and produce such records to supervisory authorities upon request.
3. **Privacy by Design:** The privacy of individuals must be considered from the outset of each new processing, product, service, or application. Moreover, only the minimum amounts of personal data that is necessary for any specific purposes should be collected and processed.
4. **Accountability:** Organizations must be able to objectively demonstrate compliance with the GDPR through appropriate technical and operational processes that have been instituted.
5. **New Data Transfer Rules:** The GDPR adds new cross-border data transfer rules to the previous directive such as certification mechanisms, codes of conduct, and exceptions. Country-specific authorization processes will no longer be needed.

EU – U.S. Privacy Shield

On July 12, 2016, the European Commission (EC) voted to adopt the final version of the EU - U.S. Privacy Shield. The Privacy Shield agreement replaces the previous agreement — Safe Harbor — which was declared invalid by the European Court of Justice (ECJ) on October 6, 2015. The new Privacy Shield is a framework to protect the rights of those in the EU whose personal data is transferred to the U.S. The Privacy Shield also brings legal clarity for businesses relying on transatlantic data transfers.

PRIVACY SHIELD IS BASED ON THE FOLLOWING CORE PRINCIPLES:

Strong obligations on companies handling data:
The U.S. Department of Commerce will conduct regular updates and reviews of participating companies to ensure compliance. Sanctions and/or removal from the list will result for those found non-compliant. A Privacy Shield company must also tighten their conditions surrounding the 'onward transfer' of data to third parties.

Clear safeguards and transparency on U.S. government access:
U.S. government entities are subject to clear limitations, safeguards, and oversight mechanisms. Further, the U.S. has ruled out indiscriminate mass surveillance on personal data transferred to the U.S.

Protection of individuals' rights:
Any EU citizen who believes that their personal data has been misused under the Privacy Shield framework will benefit from several accessible and affordable dispute resolutions channels, including free Alternate Dispute Resolution (ADR), access to Data Protection Authorities (DPAs), and arbitration.

Annual joint review mechanism:
The European Commission and the U.S. Department of Commerce will conduct annual reviews with U.S. intelligence experts and DPAs to ensure all commitments and assurances related to the Privacy Shield are functioning properly.

While some believe that Privacy Shield is fundamentally different from the previous Safe Harbor, others believe the new rules do not go far enough to protect EU citizens. In the meantime, the Privacy Shield is a valid legal basis for data transfer between the U.S. and EU. It is important to note that the Privacy Shield may be valid only temporarily as legal challenges may be forthcoming.



ASIA-PACIFIC

There are twelve jurisdictions in Asia-Pacific that have fairly comprehensive data privacy laws – these countries include Australia, Hong-Kong, India, Japan, Macao, Malaysia, New Zealand, Philippines, Singapore, South Korea, Taiwan, and China. While a half dozen privacy regulations were codified during the past thirteen years in this region, the last two years in particular have represented a significant acceleration for data privacy with noteworthy regulatory developments likened to "European-Style" privacy laws. For example, Data Protection Officers are now required in Japan, New Zealand, Philippines, Singapore and South Korea; and cross-border limitations are effective in Australia, India, Macao, Malaysia, Singapore, South Korea and Taiwan. This is particularly important for large U.S. and European companies that have set up data centers in this region.

Australia - Privacy Act 1988 (Privacy Act)

In Australia, the Federal Privacy Act regulates the collection, use, and disclosure of personal data. In March 2014, the Privacy Act was amended with the Australian Privacy Principles, which are principles intended to establish minimum standards for collecting, storing, securing, maintaining, using, and disclosing personal data.

As a general rule, entities must take reasonable steps to ensure that overseas recipients of personal data do not breach the Australian Privacy Principles. These rules are quite broad-sweeping and include the 'disclosure' of personal information (than simply the 'transfer' of personal information). Companies can be held liable when the disclosure of personal information to overseas recipients breaches the Australian Privacy Principles.

New Zealand - Privacy Act 1993

New Zealand's Privacy Act controls how 'agencies' (people or organizations, including government departments, companies of all sizes, religious groups, schools, and clubs) collect, use, disclose, store, and give access to 'personal information', defined as information about identifiable, living people. This regulation, codified in 1993, was the first to be recognized by the European Commission (EC) as providing an adequate level of data protection for EU citizens' personal data.

Japan – The Act on the Protection of Personal Information (APPI)

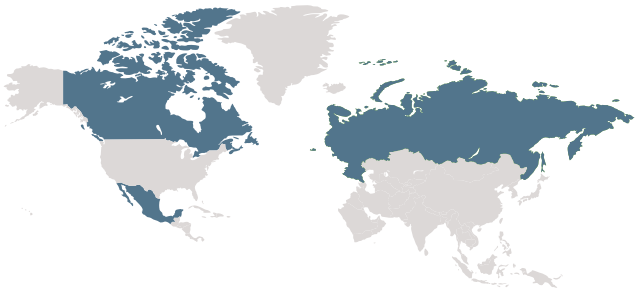
The APPI applies to the processing of personal information by data controllers and is intended to empower ministries to enforce its privacy regulations (rather than give private parties a way for a cause of action). For violations that result in personal damage to individuals, the complainant can raise a cause of action against the data controller under traditional tort or contract law.

UNDER THE APPI, DATA CONTROLLERS IN JAPAN MUST:

- Communicate the purpose and use of personal information to the data subject
- Keep collected personal information safe (I.e., from data leaks, breaches, etc.)
- Not provide personal information to third-parties, unless the data subject consents or exceptions apply
- Respond to requests by data subjects who are concerned about their personal data
- Delete personal information if it is incorrect, collected improperly, or held beyond its intended purpose

Singapore – The Personal Data Protection Act (PDPA)

The PDPA regulates both the collection and use of personal data that is collected, used, or disclosed in Singapore. Under this regulation, organization must not transfer any personal data to a country or territory outside Singapore except in accordance with the PDPA. Organizations must neither be located nor formed in Singapore in order for these regulations to apply; it applies to entities not recognized by Singapore law.



REST OF THE WORLD

Many data privacy regulations are global, reaching as far as Central and Latin America, Argentina, and Mexico to Canada and Russia. For many of these countries, their privacy laws are mainly based on their constitution; therefore, only constitutional courts may be able to review affected persons or victims of cross-border violations. Below are some data privacy regulations from these regions.

Mexico – Mexican Constitution, Article 16

The Mexican Constitution recognizes the protection of personal information as a fundamental right. Every citizen has the right to access, rectify, oppose, and cancel their personal data under these laws. And depending on whether the organization handling the data is government or private, different laws will apply – federal transparency law and data protection guidelines apply to federal entities, while the Federal Personal Data Law applies to private organizations. As for international data transfers, data controllers are responsible for ensuring that the data recipients abide by the same privacy policy principles as those within Mexico.

Canada – Personal Information Protection and Electronic Documents Act (PIPEDA)

At the federal level, PIPEDA governs the collection, use, and disclosure of personal information within the course of commercial activities. Personal information is defined as "information about an identifiable individual" and not an "identified individual"; therefore, data that can potentially identify a person is considered personal information.

Data subjects must be notified of the transfer of their personal information outside of Canada. Additionally, organizations remain accountable for information transferred to third-parties for processing whether those entities are within or outside Canada. Before data is transferred outside Canada, organizations must ensure those outside Canada meet Canadian law requirements for comparable protections via contractual means.

Russia – Federal Law No. 152-FZ on Personal Data 2006 (Personal Data Protection Act)

Article 12 of the Personal Data Protection Act regulates cross-border data transfers. Under this Act, data operators must make sure that personal data, defined as any information related to an identified or identifiable individual, is protected from foreign third-party entities with international data transfers. In order to determine whether adequate levels of data protection are proffered, data operators will look for countries included in the Strasbourg Convention or the Russian Data Protection Authority's (Roskomnadzor) own list of acceptable countries – which include Australia, Argentina, Canada, Israel, Mexico, and New Zealand.

Generally, organizations will ascertain the level of data protection provided by a foreign country before data is transferred. They can also obtain consent from the data subject or rely on data transfer agreements to ensure protections are in place.

CONCLUSION

Organizations that put additional thought and effort into data privacy strategy will reap benefits in the long term. EnCase Endpoint Security coupled with Risk Manager and Endpoint Investigator represent one of the most cost-effective and comprehensive security, compliance, and investigations suites currently available on the market. With data privacy regulations continuing to mature and hard deadlines quickly approaching, organizations should start to build internal compliance structures and frameworks that leverage technology to demonstrate compliance. It is important that your organization conducts a thorough analysis of where and how sensitive data manifests, that you review and update your cross-border data transfer strategy in light of new privacy regulations, and that you maintain this compliance going forward.

For more information regarding how Guidance Software can help with your security, compliance, and investigation challenges while remaining compliant with the data privacy regulatory landscape, contact us at (888) 999-9712 or visit guidancesoftware.com.

GUIDANCE SOFTWARE

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 35 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.

Guidance Software®, EnCase® and Tableau™ are trademarks owned by Guidance Software and may not be used without prior written permission. All other trademarks and copyrights are the property of their respective owners.