BDO

The New Era of Data Privacy: A GDPR Compliance Guide for U.S. Organizations

Table of Contents

Introduction

Businesses have grown increasingly reliant on transforming their digital capabilities, which has resulted in the need to improve data governance practices. Protecting personal data is no longer as simple as locking a file cabinet or setting up basic internal security controls. Privacy concerns are much farther reaching than in the past, ranging from bad actors to authorized users. It is critical for organizations to recognize that even authorized users may be in violation when the original intent of collecting, processing, transferring or storing personal data changes. Consider the example of the Facebook-Cambridge Analytica data scandal for a sobering reminder of the stark reputational, financial and legal consequences that can follow the misuse of personal data. Policymakers around the world are quickly modernizing data protection laws for today's fast-paced, digital environment.

On April 6, 2016, the European Union (EU) was the first to strengthen privacy safeguards when they adopted the General Data Protection Regulation (GDPR). The goal was to strengthen safeguards of EU individuals' personal data and mitigate the risk of privacy and data breaches. The regulation is the most significant overhaul to the E.U.'s data privacy policies in over twenty years and is the most comprehensive and far-reaching data privacy law that American businesses have ever encountered. Its reach extends to most companies—foreign or regional—that process the personal data of EU individuals, regardless of where it is headquartered.

The May 25, 2018 deadline to comply with the GDPR may have come and gone, but the compliance journey is just starting, as prudent and responsible data privacy governance goes beyond checking the box on implementation day. Data privacy governance is an ongoing process and a commitment to safeguarding personal and other sensitive data that your organization collects, processes, transfers or stores. The GDPR is designed with the evolving nature of data privacy in mind, and how it is monitored and enforced will change over time.

Are you ready to make a commitment to responsible data governance and data privacy practices? Get started with our in-depth guide to the nuances, complexities, and requirements of the GDPR readiness and maintenance.

EU Privacy vs. U.S. Privacy

The United States (U.S.) and the European Union take different approaches to data privacy. While the U.S. has its own fair share of protective regulations, there is no real equivalent to the GDPR, yet. In lieu of one comprehensive regulation, the U.S. has various sectoral and state-level data privacy laws. For example, the U.S. financial services and healthcare sectors—both frequent targets of cyberattacks—are subject to regulations with data privacy components through the Financial Modernization Act of 1999 and the Health Insurance Portability and Accountability Act of 2002. In contrast, the EU has one comprehensive data protection law for all 28 EU member states.

The U.S. and EU approaches to data privacy laws are prime examples of two fundamentally different structures. Since 2001 and the attacks on the U.S., Americans have been somewhat resigned—with some opposition—to the idea that the government monitors and collects their information to secure their safety. More importantly, the definition of privacy in the U.S. is flexible and there is a considerable trade-off in exchange for certain benefits and privileges. We are also accustomed to companies collecting and sharing our personal data in a relatively unrestricted manner. However, with the passage of the California Consumer Privacy Act, which goes into effect on January 1, 2020, that may change. This privacy law contains a broader definition of personal data, establishes broad rights for California residents to direct deletion of data, establishes broad rights to access personal data without certain exceptions and requires that organizations give consumers the right to know how their data is used and why it's being collected. The law also imposes more rigid restrictions on data sharing for commercial purposes.

In Europe, the legacy of the Holocaust—in which individuals were targeted based on personal information and characteristics—has left an indelible mark. European citizens see data privacy as an inalienable right with minimal exceptions. Central to the EU's definition of privacy is the notion of explicit consent: Organizations must provide data subjects the choice to decide at any time whether their personal data may be disclosed to a third party or used for a purpose materially different from the purpose(s) for which consent was originally obtained.

Balancing the GDPR regulations with U.S. regulations are a challenge for organizations of all sizes. Companies processing data have had to take a look at their risk profiles, better understand what data they collect and manage, how they handle that data and what terms and conditions are relevant for their organization and its third parties. Companies have been considering processes and practices to establish "in-country" resources to avoid transporting data across borders and risking a complaint or enforcement at the border. They may also need to engage consultants or legal counsel who have experience working with relevant data protection authorities (DPAs). U.S. companies risk facing steep fines and may be at a competitive disadvantage if they fail to comply with the new regulations.

Breaking Down the GDPR

In spirit, the GDPR is not so different from its predecessor, the Data Protection Directive of 1995 (DPD). Of the eight principles underpinning the Data Protection Act of 1998 (DPA 1998), which supplemented the DPD, seven remain largely relevant under the GDPR. The seven key principles of the GDPR, as set out in Article 5 of the regulation, include:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability principle

The accountability principle, which states that entities are accountable for complying with the seven principles and must be able to demonstrate compliance, is new.

The GDPR also increases the rights of EU individuals, explicitly outlining those enforceable rights in a dedicated chapter of the legislation (whereas under the DPD, individual rights were included as one of the eight key principles). The expanded individual data privacy rights under the GDPR are enforceable and therefore personal data must be adequately protected by U.S. businesses in order to lawfully process EU personal data[1].

PENALTIES

Data controllers or processors that do not comply with the GDPR are subject to be fined four percent (4%) of their annual global turnover or €20 million, whichever is greater. This is the maximum amount, and a tiered approach exists for lesser breaches.

TERRITORIAL SCOPE

As a U.S. company, does the new regulation apply to you? If your organization meets either of the following criteria, your data is potentially within its scope:

- A business with an "establishment" in the EU that processes personal data "in the context of its activities" (a broad test).
- A company without an EU presence when they either process personal data of individuals in the EU in connection with goods or services offered (free or paid), or they "monitor" the behavior of individuals as it takes place in the EU.

Here's a more straightforward test: Does your company deal with personal data from EU residents? If the answer is yes, then there's a good chance the GDPR applies.

1 The definition of what constitutes personal data has been broadened to include any data that can be used to identify an individual, either directly or indirectly. In addition, the special categories of "sensitive personal data" has been expanded to include genetic and biometric data.

CONTROLLER VS. PROCESSOR

The GDPR assigns different responsibilities to organizations based on their role as a "controller" or "processor" of EU data, setting specific legal requirements for each. Controllers are defined as organizations that make decisions about how personal data will be processed and used, whereas processors collect, store and process personal data for the Controller. A third category, joint controllers, is when organizations share in the determination of purpose and means of data processing and are each responsible for demonstrating compliance with the GDPR controller obligations.

Many companies are considered controllers and processors. Regardless of whether you are a processor, controller, or both, it is necessary to consider the controller's obligations.

The chart below outlines a systematic approach to ensure that you consider your obligations along with the rights of the data subject.

OBLIGATIONS AND RIGHTS

PRINCIPLES

DATA SUBJECT RIGHTS

CONTROLLER OBLIGATIONS

MEMBER STATE DEROGATIONS

OPERATIONS (PROCESSOR) AREAS

- Policies and procedures
- Technology
- Information security
- Third-party risk management
- Website activity
- Information governance/record retention
- Contract requirements
- Documentation of processing activites
- Breach notifications
- Data Protection Impact Assessment (DPIA)
- Data trasfer mechanisms

CONTROLLER OBLIGATIONS

- Identification of personal data and special categories/sensitive data
- Accountability - Documentation on compliance
- Notice
- Consent documentation and withdrawal mechanism
- Special categories of data
- Constraints and requirements for autmated decisioning
- Legitimate basis for processing
- Cross-border transfers
- Security obligations
- Data Protection Officer (DPO)
- Representatives

PRINCIPLES

- Fair, lawful, and transparent
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

RIGHTS OF THE DATA SUBJECT

- Right of access
- Rectification and erasure
- Data portability
- Right to restriction/restriction of processing
- Right to object
- Transparency
- Right to erasure

Implementing a GDPR Program

The effort required to comply with the GDPR varies among companies and requires organizations to take a more holistic approach to data privacy governance. Before embarking on your data privacy governance journey, consider:

- The nature of your data processing activities and functions
- The level of risk that these activities and functions present to an individual (data subject)
- Locations of sensitive data throughout the organization, data protection strategies and retention schedules
- The complexity of systems throughout the organization
- Existing policies and procedures that impact personal data, functions and systems

Effective data privacy governance programs are aligned with the business, operations, legal and technology. Data privacy governance programs require buy-in at the executive level along with a cultural shift in many cases. This is not one-and-done; it is an ongoing effort that requires constant vigilance. Comprehensive programs include an assessment of assets, data protection strategies and sustainability to ensure sound data management practices are followed and the ability to respond in the wake of an event or incident.

It is critical (for any privacy effort) to begin with a comprehensive evaluation that allows you to identify risks and to prioritize the remediation plan. The following list provides an easy-to-use guide to identify where gaps could exist in your GDPR program.

- Processing Activities Register
- Lawful basis for processing personal data
- Data subjects' rights and ability to comply with subject access requests
- Data retention
- Information disclosures and privacy notices
- Vendor risk management
- Appointing a Data Protection Officer
- Data Protection Impact Assessments
- Privacy-by-design and default
- Policies and procedures
- Security technology & infrastructure
- Incident response and breach notification
- Cross-border data transfers
- Training and awareness

PROCESSING ACTIVITIES REGISTER

Under Article 30 of the GDPR, both controllers and processors are required to develop and maintain detailed data registers that identify business owners, applicable systems and specific data elements, such as name and address, healthcare-related items, HR-related details and email addresses, among others. This is a challenge for U.S. organizations as it is typically the first time the company has undertaken this effort and it requires constant updates. Don't confuse this with a data map, inventory or a data flow diagram. While those are useful tools to develop your Processing Activities Register, the level of detail in the register is different.

Below is an outline of the differences between a Processing Activities Register for Controllers and Processors. Note that the requirements for a processor are slightly less onerous.

Requirement	Controller	Processor
Type of processing activity	✓	✓
Purpose of processing	✓	
Contact information	✓	✓
Categories of data subjects	✓	
Recipients of the data	✓	
Transfers of personal data	✓	✓
Retention periods	✓	
Time limits for erasure	✓	
Security measures	✓[2]	✓
Data Protection Officer		✓
Categories of processing		✓

Data registers are living, breathing records that require regular updates. Typical questions that assist in the development of a Processing Activities Register include:

- What is the reason for data processing, and is it justified?
- Have we obtained permission from the data subject and have we been transparent about the way in which we are going to use the data?
- Do we need all the data we are collecting?
- Are we only storing data that is required for those purposes?
- How do we ensure that the data is accurate and up-to-date?
- How long do we retain data, and is that an acceptable retention period?

Building and maintaining a Processing Activities Register is now a requirement under the GDPR—but it will also help to develop data privacy governance as a foundation for your organization.

LAWFUL BASIS FOR PROCESSING PERSONAL DATA

Organizations must establish a lawful basis to process EU personal data. The basis must be decided and documented before processing begins. The lawful bases allowed under the GDPR include:

- Consent
- Fulfilling a contract that the data subject is involved in
- Complying with a legal obligation
- Protecting public interest
- Protecting the vital interests of data subject or another person in a situation involving life or death
- Fulfilling a "legitimate interest" of the organization, except if the data processing threatens fundamental rights and freedoms of an individual, particularly a minor

Apart from personal data the GDPR also defines sensitive personal data as any information identifying an individual's race, ethnicity, sexual orientation, religion or political affiliation, or health, genetic or biometric data. These forms of data require more scrutiny when determining their lawful bases for processing[3].

2 Outlined in Article 32(1).

3 Special categories are defined under Articles 9 and 10. Specific conditions for processing special categories are listed in Article 9(2) and expanded on in Schedule 1 of the Data Protection Act 2018.

PROTECTING DATA SUBJECTS' RIGHTS AND FACILITATING ACCESS REQUESTS

Given that the GDPR provides individuals certain rights, controllers and processors must be prepared to afford those rights to the individual. Upon completion of the Processing Activities Register, the organization should develop a process to handle, record and manage requests. This is no easy task. Based on our experience, we have found that organizations struggle with this part of the puzzle. Bear in mind that it is critical to implement a process that not only provides some level of automation, but also allows the organization to comply with other regulatory requirements. Also, it is important to remember that companies have 30 days to comply with these requests and can request a 60-day extension in some cases. The following visual is a methodology to implement sound subject request practices.

DATA RETENTION RULES

Data minimization is a key element of the GDPR, which requires companies to better manage data across the organization. Data must be deleted when it is no longer needed. If your company has an information governance program that allows for standard and organization-wide retention, storage and proper disposition practices of data, then you are one step ahead of the game. If you do not have a current information governance program, then a good first step is to identify the most sensitive sources of personal data to ensure that you are not retaining this information any longer than required.

Key data retention principles[4] to consider include:

- Determine who is accountable for maintaining records schedules related to each category of data
- Align records schedules with business, operational and legal practices – ensure that you are not deleting data (for erasure requests) that you are required to keep by law
- Identify the country or region with the shortest and longest retention periods to determine the least amount of time you are required to maintain the record
- Ensure that the records keeping program protects personal records and data
- Identify and articulate potential legal concerns due to non-compliance with either the GDPR and/or the records keeping program
- Document organizational practices and ensure that data is properly categorized, including public, private, confidential and company secrets
- Determine safeguards during the disposition processes – shred documents that require shredding, destroy hard drives in a proper manner that require destruction
- Update and maintain current retention schedules and policies
- Ensure that there is transparency about the organization's data retention practices – internally and externally

With the GDPR in effect, organizations will need to leverage a mixture of data minimization, deduplication, redaction, and more sophisticated artificial intelligence-driven data analysis to limit data collection to only the most critical information. These case-by-case balancing acts can be nerve-wracking, and many are counting on an earnest, thorough attempt to filter out all noncritical sensitive data to the extent possible to earn favor with regulators. In the end, a company may be forced to decide which legal risk to take—violating data protection laws or non-compliance with a U.S. subpoena or discovery requirement.

But to make the right decision for your business, you must have a full understanding of the consequences and prove best-effort compliance with both sets of laws.

INFORMATION DISCLOSURE AND PRIVACY NOTICES

Inherent to the GDPR's individual rights and its notion of "fair and transparent processing" is the right for individual data subjects to be informed about how, why and for how long their personal data is being used, as well as where it goes and who receives it. To uphold this right, organizations are required to proactively provide individuals with this information in a transparent, concise and easily accessible way, using clear and plain language. These "privacy notices" must be provided at every point that an individual's personal data is obtained. In addition, organizations must regularly review and update their privacy notices that are available to the public. If the controller wishes to use an individual's information for additional purposes beyond the original intent, the individual must be notified before the controller can move forward with the new processing activity.

Now that you know what personal data exists throughout the organization, the organization is able to develop processes to determine what information needs to be communicated to data subjects, and how this information can be delivered. In all cases, it is important to develop a robust privacy center or privacy notice that is available to the public. Privacy centers that are typically posted on your website include:

- Personal Data that is collected, definitions and how it's used
- How data is collected, and how long it's maintained
- An outline of Cookie preferences
- Disclosure of personal data
- Practices when sharing data with third parties or advertisers
- A security overview
- The ability to opt-out of marketing-related activities
- How the data subject can access, change, request a copy of or delete their personal data
- The organization's handling of sensitive data
- The use of data provided by minors
- Compliance with Privacy Shield
- How to contact the privacy team or the Data Protection Officer
- Other related information that is not included in the one of the above categories

4 ARMA Generally Accepted Recordkeeping Principles®

Privacy notices range in length and complexity based on the organization. Choose the options that best fit your company and your customers to ensure that you are transparent and clear about the organization's intentions as it relates to their personal data.

VENDOR RISK MANAGEMENT

Data controllers and processors are liable for the actions of their vendors that process personal data[5], using only those processors or sub-processors that provide "sufficient guarantees" they are taking adequate measures to protect individuals' privacy rights. In other words, controllers should view their third-party relationships as extensions of their own business and hold them to the same standards. Under GDPR organizations are required to demonstrate appropriate due diligence and take proactive steps to ensure their vendors are prioritizing privacy and able to fulfill the requirements under the GDPR directly applicable to processors.

As a starting point, organizations will need to identify all existing and future third-party vendor relationships and map those relationships against data flows to understand what level of access they could have to personal data from individuals in the EU. Compliance can be measured by performing privacy risk assessments with each vendor or sub-processor. Vendors' data privacy policies and procedures should be closely examined, as should their compliance practices. The vendors then must demonstrate a thorough understanding of their direct GDPR requirements as well as the controller's responsibilities—and the consequences of running afoul of those rules. Existing contractual obligations may need to be modified to include all compulsory details and terms under the GDPR. Processors cannot engage other processors without the controller's authorization and must also have a written contract with the sub-processor that conforms with the GDPR guidelines.

The vendor management process, however, does not end after the contract is signed or the vendor risk assessment is concluded. The key to successful vendor risk mitigation is that it is a continuous process—not something that is simply conducted upfront and then forgotten. Controllers must diligently monitor risk and review internal controls with service providers to ensure they remain compliant in the changing environment. Adopting a formal vendor management program—or upgrading your existing program—has never been more important.

APPOINTING A DATA PROTECTION OFFICER

Under certain circumstances, controllers or processors may be required to designate a Data Protection Officer (DPO). The requirement applies if your organization is a public authority or if you engage in certain types of processing activities, including:

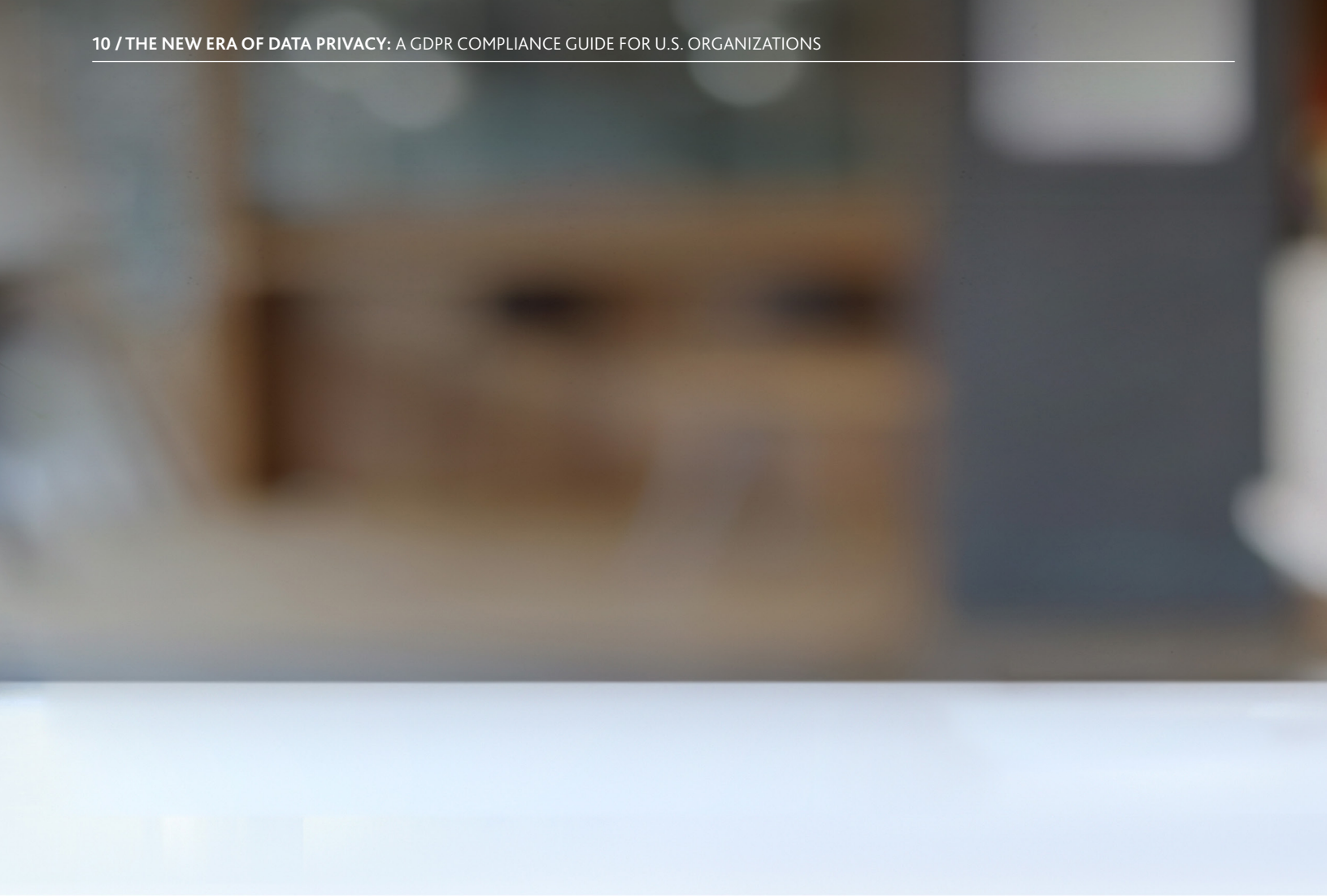
- Systematic monitoring at a large scale
- Processing special categories of personal data, as outlined in Article 9
- Processing of personal data related to criminal offenses, as outlined in Article 10.

The DPO selection process is not an easy task as the organization must ensure that the DPO:

- Demonstrates expertise in data protection laws and practices
- Has the ability to act in an important advisory role, responsible for the oversight of GDPR training and awareness programs
- Is able to monitor ongoing GDPR compliance
- Can act as the primary contact for Supervisory Authorities and data subject requests

Some companies are appointing internal personnel to serve as the DPO. Before committing to an internal individual, ensure that they are able to meet the aforementioned requirements, and that they will be able to report to the highest possible level of management. Regardless of whether your organization is required to appoint a DPO, ensure that the company has a person, or persons, that is responsible for data privacy governance.

5 Article 28.



DATA PROTECTION IMPACT ASSESSMENT

Data controllers are required to conduct a Data Protection Impact Assessment (DPIA)[6] for any data processing that poses "high risk" to individual data subjects' rights and freedoms. A DPIA is a conscious and systematic effort to assess the privacy risks to individuals in the collection, use and disclosure of their personal data, and determine whether the level of risk posed is acceptable. Put simply by the Article 29 Data Protection Working Party (WP29), "a DPIA is a process for building and demonstrating compliance."

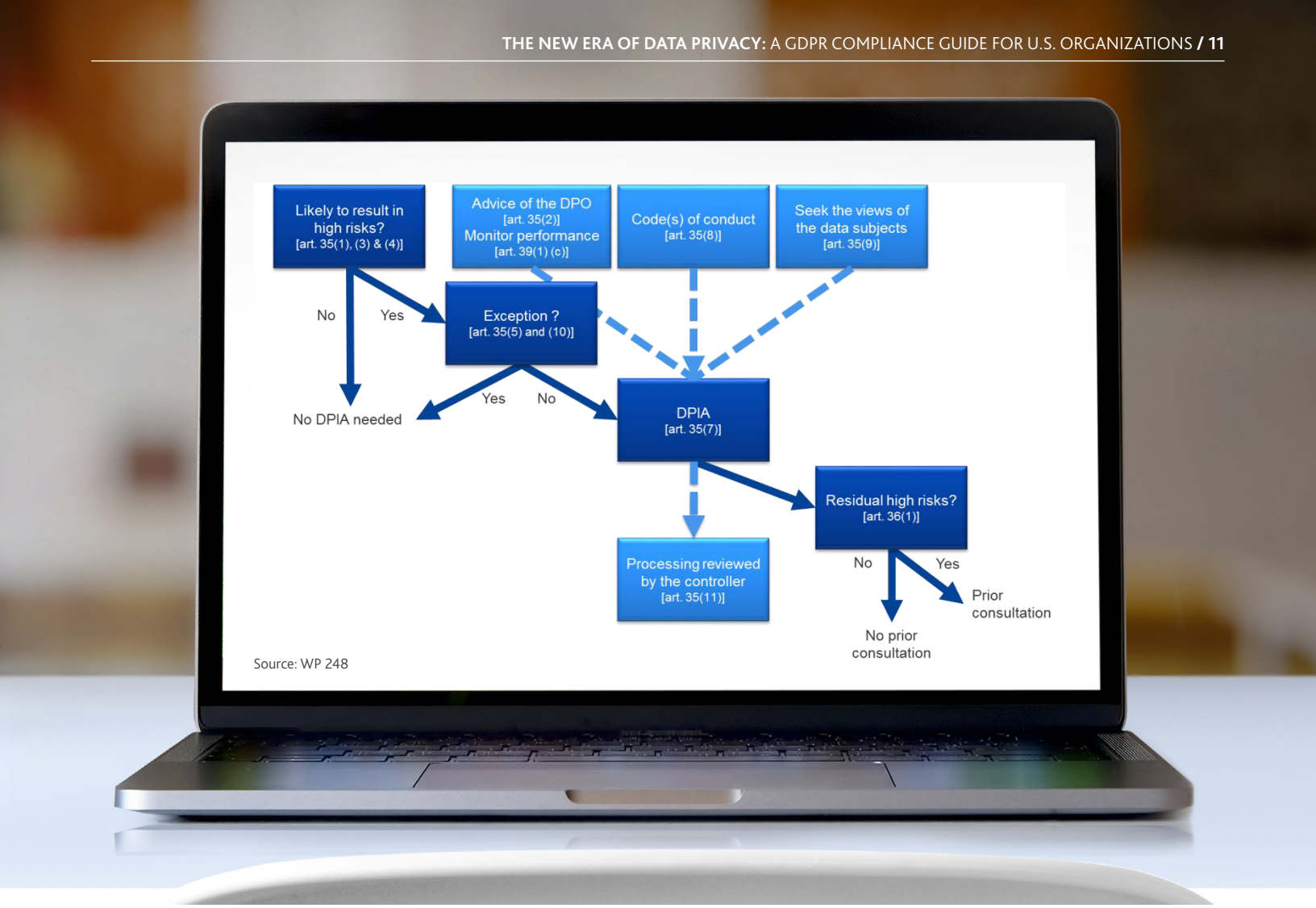
Central to privacy design, a DPIA should be carried out as early as possible, at the onset of a new process or development of technology, to ensure privacy risks are adequately addressed and any problematic outcomes from the assessment are mitigated prior to commencing the process. That does not, however, mean that processing activities already underway are exempt from the DPIA requirement.

A DPIA is **not** necessary for every processing activity; it is only mandatory for those activities that pose "high risk."

The GDPR and subsequent guidance from the WP29 lay out specific—but not exhaustive—circumstances in which a DPIA is legally required, including:

- The use of new data processing systems or technologies
- Evaluating or scoring, including profiling and predicting
- Automated decision-making with legal or similar significant effect
- Processing special categories of personal data as well as data related to criminal offenses
- Data processed on a large scale (not yet clearly defined)
- Systematic monitoring of a publicly accessible area (such as CCTV)
- Data concerning "vulnerable data subjects," such as children, the elderly, the mentally ill—or any case where there is an imbalance of power between the controller and data subject
- Transferring data across borders outside the EU

6 Article 35.



To determine whether a processing activity or set of similar processes requires a DPIA, organizations should start with a data audit to understand what data you have and inventory sensitive data that could qualify as "high risk." A data mapping exercise can then help you understand and document the business processes and applications that may use this data and therefore may require a DPIA. Existing Privacy Impact Assessment methodologies to assess risks can be used as a starting threshold.

While the GDPR does not mandate a specific framework, a DPIA must at a minimum include:

1. A description of how and why the data will be processed
2. An assessment of the necessity and proportionality
3. An assessment of the risks to individual data privacy rights and freedoms
4. The measures to address these risks

Organizations are also required to formally seek out the advice of their designated DPO and document their advice as part of the DPIA process. The DPO must also sign off on the DPIA outcomes.

Keep in mind that a DPIA is not intended to be a one-and-done process; it is meant to be continuously updated as problems are identified and addressed. And in some cases, it can even be a competitive advantage. Software developers and manufacturers, for example should consider conducting DPIAs on their products to determine the end-user privacy risks to personal data and mitigate those risks as part of the software or product development life cycle.

PRIVACY-BY-DESIGN AND DEFAULT

The GDPR's Privacy by Design and Privacy by Default principles are meant to ensure that stronger privacy controls are embedded in a system's core functionality from the very beginning. At the policy level, "Privacy by Design" requires entities to account for the protection of any consumer data they use throughout the entire lifecycle of the development of a product or service. "Privacy by Default" automatically affords consumers the principle of least privilege when it comes to the personal data newly acquired products or services can access from them. Businesses are required to adopt appropriate technical and organizational measures to ensure they only process personal data to the extent necessary, and by extension, limit the amount of data collected, the duration for which it is retained and who has access to it. For products and services to gain access to more of their personal data, consumers will have to manually approve that access.

Privacy by Design is not a new concept—in fact, it is a central component of the Federal Trade Commission's (FTC) consumer privacy framework, which states: "Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services." The key difference is that the GDPR makes adherence to the Privacy by Design framework a legal and enforceable requirement.

But implementing the GDPR's Privacy by Design and Default policies is more than a compliance exercise; it requires a philosophical shift in mindset from a reactive to a proactive approach to data privacy, with the rights and interests of the individual user at the center.

THE 7 FOUNDATIONAL PRINCIPLES OF PRIVACY BY DESIGN

1. Proactive Not Reactive; Preventative Not Remedial

Anticipate and prevent data privacy incidents, and address privacy risks before they materialize.

2. Privacy as the Default

Privacy is built inot the system by default, requiring no action on the part of the individual to protect their privacy.

3. Privacy Embedded Into Design

Embed privacy into the design and architecture of IT systems and business processes as a core functionality.

4. Full Functionality – Positive-Sum, Not Zero-Sum

Privacy protections should not and do not need to come at the expense of security or functionality.

5. End-to-End Security – Lifecycle Protection

Anticipate and prevent data privacy incidents, and address privacy risks before they materialize.

6. Visibility and Transparency

Provide assurance to all stakeholders – users and providers – that data is being used in accordnace with stated principles and obectives – subject to independent verification via a compliance and redress mechanism.

7. Respect for User Privacy

Take a user-centric approach to data privacy, prioritizing individual privacy interests, communicating effectively and providing user-friendly options.

POLICIES AND PROCEDURES

The GDPR requires organizations to examine their information governance practices in a detailed and deliberate way. Because the GDPR exists in a complex data privacy ecosystem, part of the challenge for U.S. organizations is to harmonize policy and procedural requirements with domestic and sector-specific requirements. As organizations tackle compliance, it's vital to align GDPR-related privacy initiatives with existing policies and procedures, including the AICPA's data privacy framework, and industry-specific rules like HIPPA and GLBA. Companies that have not implemented an established privacy framework may consider creating policies and procedures using the GDPR's requirements as a starting point.

When evaluating the appropriate policies that your organization should implement, consider whether the policies consistently meet the following standards:

- Governance: The policy clearly addresses the governance, compliance and regulatory requirements of the organization;
- Policy statements: The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed;
- Policy statements: While these vary, the entity must maintain accurate, complete and relevant personal data and should ensure that the policy outlines specific uses for personal data along with retention, destruction and change control requirements.

Typically, when you are considering whether your policies meet the requirements outlined by specific countries or sectors, it is important to have consistent policies across the organization. Oftentimes, companies have not reviewed their policies in years and do not have consistent definitions across the organization. Some global organizations define personal data in up to three or five different ways. Ensure that definitions are consistent—oftentimes this can be solved by including a glossary that is linked to each policy.

SECURITY TECHNOLOGY AND INFRASTRUCTURE

All organizations are required to put in place technical and organizational measures to ensure an appropriate level of security, including by implementing a process to regularly test and assess the effectiveness of such security measures[7]. When assessing the appropriate level of security, you must consider risks that data processing presents, particularly from accidental or unlawful destruction, loss, access to or disclosure of personal data.

For most organizations, compliance with this provision means confirming their existing cybersecurity programs are GDPR-ready and assessing the effectiveness of their current security and IT controls. While conducting a privacy risk assessment, you should be able to identify what additional security measures are needed to appropriately address the appropriate levels of risk. Reviewing results from the following security tests can assist in conducting a privacy risk assessment:

- External Vulnerability Assessment and Penetration Test (VAPT)
- Internal Vulnerability Assessment and Penetration Test (VAPT)
- Web application review
- IT operations controls assessment
- Payment Card Industry (PCI) readiness
- Wireless security assessments
- Bring your own device (BYOD) security assessments
- Social engineering tests
- Network and security device configuration reviews
- Personally identifiable information (PII) reviews
- End-user device configuration reviews
- Host assessments
- Third party/service provider risk assessments
- Cloud services assessments
- Mobile device assessments
- Dark web reconnaissance

Each company is unique and requires different levels of security tests. Regardless of the size of your organization, ensure that data privacy is at the forefront of any security test performed for the company.

7 Article 32.

INCIDENT RESPONSE AND BREACH NOTIFICATION

One key area where the GDPR is stronger in scope and enforceability than its predecessor is the handling of privacy breaches. The regulation defines a "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." If a breach should occur, the data controller must notify its relevant DPA within 72 hours of awareness, when feasible. It must also notify the affected data subjects if the breach is likely to result in risk to individual rights and freedoms "without undue delay" (notification does not have to occur if the breach does not). The GDPR includes content requirements for notifications and sets forth limited exceptions to the notification rules.

Data processors are also required to notify **their** customers—the controllers—without undue delay. The controller is responsible for documenting any privacy breaches and the remedial actions taken in order to prove GDPR compliance and illustrate sufficient measures were taken to protect the personal data.

A precursor to the breach notification reporting requirement is that you must have a comprehensive incident response plan in place, including breach detection and internal reporting mechanisms. All incidents must be formally recorded in a breach register and analyzed as part of a comprehensive incident response management system—regardless of whether notification is required. To get into compliance, you may be able to leverage your current incident response management system with some small tweaks. At a minimum, organizations should develop a defined process with clear roles and responsibilities to effectively respond to a breach within the 72-hour deadline.

Critical aspects of developing sound incident response and data breach notification processes include:

- Consistent and current incident response program that includes policies, procedures, roles and responsibilities, as well as communications plans
- Consistent definitions across the organization that includes the definition of an event, an incident or a breach
- Direction to teams that an incident has occurred, and the steps required in the event that they suspect that this requires further investigation
- Contracts with outside counsel, forensic and cyber investigative experts, and PR firms that specialize in this area
- Internal training to identify suspicious activities
- Steps to minimize further threats or exposures, and a process to remediate the current situation
- Notification practices, such as outsourced data breach notification companies, credit monitoring contracts, and the like required after a breach has occurred

In the event you suspect that an event is actually an incident, following is a high-level process to organization your efforts.

IDENTIFICATION

- Location of the incident
- How was it discovered?
- Other areas compromised?
- Scope of the impact
- Have sources been identified?
- Business impact

CONTAINMENT

- Short-term containment (is problem isolated/ are systems isolated?)
- System-backup (evidence collection, imaging)
- Long-term containment (system off-line)

ERADICATION

- Re-image and update patches, harden system(s)
- Removal of malware and artifacts from system(s)

RECOVERY

- When can system(s) come back online?
- Have systems been prepared to thwart future attacks?
- What testing, monitoring solutions are going to be used for future?

LESSONS LEARNED

- How can we prevent this in the future?
- Incident Report
  - Who?
  - What?
  - Why?
  - How?
  - Where?
  - When?
- Implement preventative measures

INCIDENT RESPONSE AND REMEDIATION

Remember, your organization's goal is to reduce risk to the individual. By instituting sound incident response and breach notification practices, you will be one step closer to complying with the GDPR.

CROSS-BORDER TRANSFERS

U.S. organizations may need to transfer personal data to or from the EU for a variety of reasons: to facilitate e-commerce, deliver digitally-enabled services, glean customer intelligence, monitor and manage global operations, implement compliance procedures or conduct an investigation or litigation, just to name a few. In fact, cross-border data flows between the U.S. and EU are the highest in the world. To put it into perspective, in 2015, the EU accounted for $70 billion of the United States' $161.5 billion trade surplus in digitally deliverable services.

Currently used by more than 3,300 organizations, the E.U.-U.S. Privacy Shield agreement provides an adequate legal mechanism to transfer personal data from the EU to the U.S. U.S. organizations that choose to self-certify under Privacy Shield voluntarily submit to enforcement by the FTC, Department of Commerce and EU Data Protection Authorities (DPAs). Self-certification under the Privacy Shield is relatively easy; **compliance** is a different story, and in some cases, may prove more burdensome than alternative legal mechanisms. Organizations need to consider Privacy Shield certification carefully since it has come under attack numerous times, and its future is precarious. Recently, the European Parliament passed a resolution calling for its suspension. However, only the European Commission has the power to suspend the Privacy Shield mechanism.

Organizations may also consider appropriate safeguards such as requesting DPA authorization, instituting binding corporate rules—which only allow for intra-company data transfers—or making use of standard contractual clauses (SCCs).

In the absence of the Privacy Shield or another appropriate safeguard, organizations also can use the following derogations to transfer personal information from the EU to the U.S.:

- Explicit consent
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
- For reasons of public interest
- For the establishment, exercise or defense of legal claims
- To protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
- The transfer is made from a register which according to Union or Member State law is intended to provide information to the public

Another alternative? Some organizations have opted to host their customer data in EU data centers to circumvent the need for third country transfers altogether.

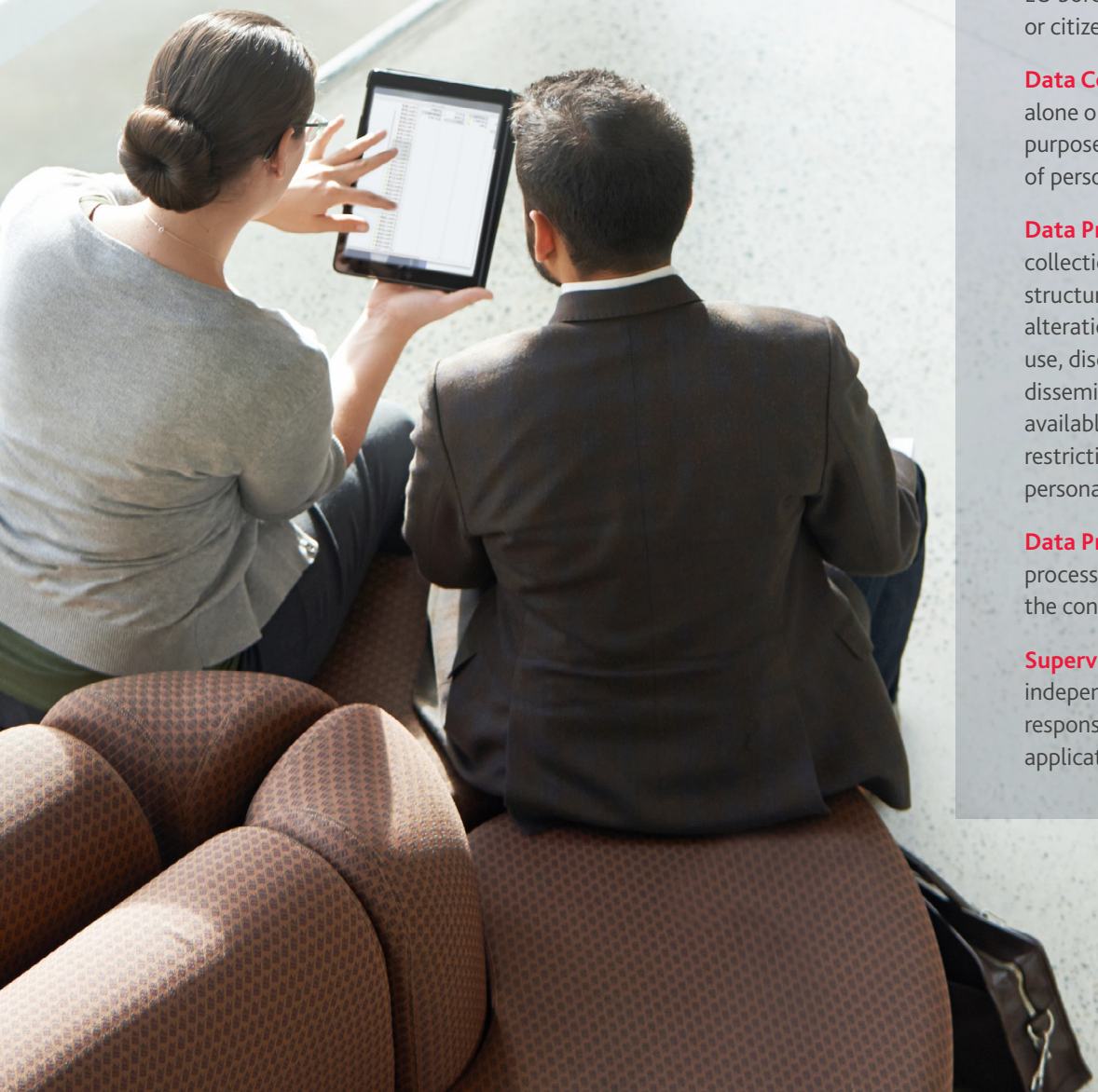
TRAINING AND AWARENESS

As a part of GDPR compliance plans, organizations should also prioritize educating employees about the updated data privacy programs and how actions at the individual level contribute to the organizations' overall privacy health. As international data privacy standards continue to evolve, more stringent requirements are in the not-too distant future. Monitoring for additional regulatory changes and going beyond the basic requirements is a prudent practice for all organizations to adopt.

Training programs are available in a variety of methods, including on premise or online. In many cases, the organization is likely disparately located, which prevents the ability to provide on-premise training. However, do not forget to train-the-trainer. In certain circumstances your organization may opt to elect privacy training champions to deliver important messages in person and to better prepare the workforce to assist with GDPR compliance.

Moving Forward in a Post-GDPR World

The GDPR is more stringent than any data privacy regulation we have in the U.S., but it's just a matter of time until U.S. regulators play catchup. It behooves every organization—whether they touch EU personal data or not—to regularly review how information is managed to maximize its value and minimize risk. The GDPR sends a clear message: Don't put information governance and data privacy on the backburner.



GDPR GLOSSARY OF TERMS

Personal Data: Any information related to an individual that can be used directly or indirectly to make identification.

Sensitive Data: This relates to information concerning a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life or details of criminal offences.

Data Subject: Open to interpretation. Applies at minimum to all EU citizens. In the broadest interpretation, "data subject" refers to all individuals within EU borders, regardless of nationality or citizenship.

Data Controller: The entity which, alone or jointly, determines the purposes and means of the processing of personal data.

Data Processing: Includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

Data Processor: The entity which processes personal data on behalf of the controller.

Supervisory Authority: The independent public authority responsible for monitoring the application of the GDPR.

CONTACT

KAREN SCHULER
National Data & Information Governance Leader
kschuler@bdo.com

OLIVETTE JOSEPH
Senior Associate, Data Privacy
ojoseph@bdo.com

People who know Cybersecurity, know BDO.