Practical Defensibility for GDPR

1. Sensible Compliance for Tougher European Privacy Laws

The European Union's new General Data Protection Regulation (GDPR) takes effect in May 2018. The new rules seek to better protect the personal information of individual EU citizens by updating and strengthening data handling and movement by organizations doing business in member nations.

While designed to push back against the rising influence of global social media, cloud computing, and search giants, GDPR's breadth also creates compliance challenges for organizations of all sizes. The tougher new regulations require that any company conducting any sort of business in the EU must prove it has adequate processes in place to manage and protect EU residents' personal data, or risk fines of up to 4% of annual revenue.

Most large companies have been aware of the impending deadline since early 2016 and many have been building a compliance program for months. Some mid-size companies have only recently started to assess their compliance obligations. However, with deadlines fast approaching, many organizations in both categories are realizing that there is more complexity to the readiness efforts than initially anticipated. Often the challenges stem from the need for business unit leadership, legal, and IT to work cooperatively to design and implement a GDPR compliant program. Disputes over budget allocation, practicality of required controls, accountability for program design and management have become commonplace and are hampering efforts to achieve a defensible state of readiness by the May 25 deadline.

24% of respondents in a new ISACA global survey reported their organizations are taking a "wait-and-see" attitude about how GDPR will impact their organization. 24% are unsure of what progress has been made to prepare for the new regulations.
Source: "Better Tech Governance is Better for Business", 2017.

What's more, many organizations lack the understanding, staffing, and experience uniting the Legal, IT Security, Privacy, and Information Governance functions needed to successfully plan, scope, design, execute, and manage ongoing compliance.

In this white paper, we outline a practical, common-sense approach to GDPR compliance. While there's no one-size-fits-all formula, focusing on a few key, actionable elements and your organization's unique risk profile helps build a defensible GDPR-compliant program that can withstand regulatory scrutiny without being too complex, too expensive, and ultimately, unsustainable over the long run. Implementing a common-sense program dramatically reduces the risk of an unfavorable enforcement action that can bring large fines, legal fees, mitigation costs, and costly damage to reputation and brand resulting from noncompliance. More importantly, it keeps your organization safely engaged in one of the most important markets in the world.

2. Understanding GDPR and Requirements

The first step in creating a sensible, defensible plan for your organization is understanding the basics of the new regulation.

GDPR (EU) 2016/679 replaces EU's Directive 95/46/EC, which has provided data protection guidance since 1995. Passed after years of discussion, debate, and lobbying, GDPR contains 99 articles with 80% new requirements reflecting major changes over the last two decades in technology and the management of private data.

Most significant are the introduction of the individual's "Right to be Forgotten" (removal of personal data) and "Right to Portability" (freedom to move data across services). Although these provisions technically apply to every organization subject to GDPR, unless you are a media company or search engine operator, they're unlikely to cause major disruptions or concerns.

For the average U.S.-based organization doing business in the EU, several new requirements and restrictions for handling personal data and notification of data breaches should be top-of-mind:

Records of Processing Activities – Companies are required to identify and clearly document all activities involving the processing of personal information for EU data subjects.

Privacy Impact Assessments/ Privacy by Design – Companies must implement a program under which they will conduct a formal analysis of data protection and privacy implications of any new business process or system.

Data Security Controls – Protecting personal information while under a company's control is a key element of GDPR. Access controls, use of encryption, and pseudonymization as well as the maintenance of adequate technical security measures will be scrutinized under GDPR.

Data Transfer Restrictions – Like the prior regime of Directive 95/46/ EC, organizations must safeguard personal data transferred outside the EU by relying on one of several options: adequacy, consent, binding corporate rules, or other contractual provisions.

Data Breach Notification – Companies must notify an EU data protection authority within 72 hours of a data breach event that compromises personal information of an EU member-state citizen.

Data Protection Officer – Any company that conducts "regular and systematic monitoring of data subjects on a large scale," or processes particularly sensitive personal information as defined in Article 9, must appoint a Data Protection Officer to advise on and monitor GDPR compliance, and serve as primary interface with regulators and data subjects..

Bottom line: GDPR requires that organizations doing business in the EU must ensure that IT systems, staffing, policies, and contracts comply with these new rights and responsibilities. Whether your company does business with just one EU citizen or in one EU location, your enterprise must comply—no matter where it is headquartered or with whom you do business.

Failure to have a defensible compliance program in place by the GDPR effective date of May 25, 2018, can bring fines of up to 4% of a company's gross global revenue (an estimated penalty of $480 million for a Dow Jones-listed company).

3. Developing a Defensible Plan

We recommend the following foundational steps as a simple way to create a common-sense action plan for GDPR compliance:

UNDERSTAND AND INTERPRET KEY DEFINITIONS

For most organizations, assessing their GDPR compliance obligations should begin by determining what data they are collecting, and how such data is used. We recommend starting with a clear understanding and interpretation of two key EU definitions

“Personal Data” is defined as any information relating to a natural person (“data subject”) who is identified or identifiable by a name, identification number, location data, online identifier, or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.

“Processing Activity” is defined as any operation or set of operations performed on personal data or sets, “whether or not by automated means, such as 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.”

The first task for many organizations should be to identify the circumstances under which personal data is collected, including through web forms or other marketing mechanisms, collection of employee or contractor data, and customer information gathered for purposes of delivering a service. Consider collecting this data by conducting a data use and security audit. To be clear, companies are not prevented from collecting such information, but must follow certain restrictions in the GDPR. (See box below)

Most organizations engage in several different types of processing activities. Employee data processing for HR purposes, customer data processing involved in fulfilling orders and carrying out contractual obligations, marketing data used in prospecting, and new business development efforts are all common categories of data processing companies will need to closely examine for GDPR-compliance issues.

Data Do’s – Under the GDPR, personal data must be:

- Collected for specified, explicit and legitimate purpose.
- Accurate and up-to-date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purpose.
- Processed in a manner that ensures proper security of data, including protection against unauthorized or unlawful processing, and against accidental loss and destruction.

MAP DATA

Once an organization has identified processing activities as defined by GDPR, the next task is to map where and how personal data flows and is stored in its environment as well as with third party contractors. Doing so enables you to answer questions of key concern to regulators, including data security, who has control, and whether personal data will be transferred outside the EU.

Structured data stores such as marketing databases, personnel records, and customer data should be relatively easy to survey and identify. For these data types, we recommend that an organization conduct an honest assessment of the business value of retaining and/or processing such data. Many organizations retain far more personal data than they can use. The GDPR requires organizations to apply a more conservative standard to the decision to keep personal information, since the penalty for misuse or loss is so significant.

The bigger challenge will come in identifying personal data contained in unstructured data sources, such as email. User awareness is an important piece of a GDPR compliance readiness effort. Users must be made aware of the consequences of sharing personal data belonging to EU citizens and discouraged from doing so. Companies should also consider implementing a mechanism to monitor email. Assessing the proper role for encryption and pseudonymization is a critical step in the process as well.

DESIGN A PROGRAM BASED ON YOUR RISK PROFILE

Identifying and locating personal data restricted by the GDPR provides you with a workable risk profile that will set the scope for efforts to implement defensible processes designed to protect and manage that affected data. The GDPR offers little guidance about specific measures that organizations must implement to become compliant. This vagueness presents both opportunity and a temptation for affected organizations.

In many cases, companies with a mature information security program will be able to make minor adjustments to prove that all identifiable EU citizen information is adequately protected. For companies less confident that their existing information security program can withstand scrutiny, the advent of the GDPR is a great opportunity to conduct a thorough review of security controls, with a focus on personal data. An emphasis on security basics such as access controls, patching, and vulnerability management, along with an examination of incident detection and response capabilities, will yield positive results.

Similarly, organizations that already have in-place incident response program based on best practices should be able to adapt to new GDPR reporting requirements, including 72-hour notification, with relative ease and modest expense. If you are one of the many U.S. organizations lacking such a workable program, the new EU regulations offer a powerful added impetus to create one.

On the other hand, we strongly advise organizations to avoid being overly influenced by the growing volume of fear, uncertainty, and doubt (FUD) around GDPR that is prevalent in the industry today. Many vendors and consultants are heavily promoting expensive new GDPR services and products. Organizations should be aware of several potential, serious drawbacks of large and complex “green field” solutions.

First, many offerings depend on cookie-cutter “methodologies,” templates, and armies of consultants to create GDPR frameworks that are massive overkill for most mid-market organizations. Second, many providers come from a distinct IT background and lack deep experience collaborating with Legal, Compliance, Privacy, and other key GDPR stakeholders.

As we’ve noted, effective (and cost-effective) GDPR response must be driven by an organization’s unique risk profile and existing capabilities. Very few companies need the world-class, heavy-duty frameworks needed by Facebook, Google, Twitter, and other global giants. Most organizations will be far better served by a more personalized, logical approach that distills the massive GDPR to its core actionable elements, and fully uses existing data protection and management processes and capabilities. The resulting protections will be compliant, properly scoped and, most importantly, appropriately defensible for your business situation.

4. How UnitedLex Can Help

UnitedLex GDPR Readiness Consulting Services provide leadership and support for your internal compliance efforts. UnitedLex supplies as much – or as little – support as you need. Rather than air-dropping an army of consultants with checklists at your doorstep, UnitedLex integrates with your existing team and leverages prior investments in process and/or technology to ease the task of GDPR compliance. We will not insist that you implement a particular technology or set of policies, but will instead help practically apply the GDPR framework in your environment.

Our services include:

- **Identification and Documentation of Processing Activities.** Using a combination of automated survey tools and stakeholder interviews, UnitedLex can help you identify and document processing activities involving EU personal data and map the location of protected data types.
- **Privacy Impact Assessments (PIAs).** The UnitedLex team can design and conduct PIAs across your organization to identify areas where compliance efforts are needed.

- **Technical Security Controls Review**. UnitedLex security and privacy experts can engage in a rapid but thorough review of existing security and privacy controls to highlight gaps and weaknesses that need to be addressed.
- **Policy and Procedure Review and Remediation.** Certified Privacy Professionals can review existing documentation and assist in developing and/or enhancing policies to enable you to show compliance.
- **Contract Remediation and Data Processing Agreements.** UnitedLex contract experts can help you quickly and cost-effectively review your existing vendor and other business contracts, identify GDPR-compliance remediation steps, and negotiate new terms as well as Data Processing Agreements to put you in a defensible position.
- **Data Subject Access Requests.** UnitedLex can assist you in designing a process for responding to requests from EU data subjects to access, modify, and/or delete their personal information. UnitedLex offers a subject access request managed service to reduce the burden on your internal teams.
- **Incident Response Readiness.** The UnitedLex digital forensics and incident response team can help ensure that you will be able to meet the GDPR's 72-hour breach notification requirement and be prepared to mitigate potential impact of a security incident.
- **Employee Awareness and Executive Briefings.** Ensuring that your employees understand the company's obligations and risks under GDPR is a critical part of your GDPR-readiness. UnitedLex privacy training experts can work with you to design and implement a program that is specific to your organization. UnitedLex can also help you stay current by providing regular briefings to your executive team.

UnitedLex brings you deep understanding of the convergence of Legal, IT Security, Privacy, Information Governance, and Compliance functions necessary to achieve sustainable GDPR compliance.

For information, contact UnitedLex at info@unitedlex.com.

About UnitedLex

UnitedLex—the world's leading enterprise legal services provider—drives transformation throughout the entire legal ecosystem. UnitedLex was founded in 2006 with a singular mission to improve the performance of leading corporations, law firms, and academic institutions. Since then, more than 2,700 attorneys, engineers, and consultants across four continents have deployed innovative service models and digitally powered solutions that deliver unparalleled business impact resulting in risk mitigation, efficiency improvements, and cost optimization for clients around the world.