Securing Privacy: Understanding the Impact of GDPR
The deadline to comply with the General Data Protection Regulation (GDPR) was **May 25, 2018**. This regulation affects any organization that processes and/or handles the information of European Union citizens. Do you understand the impact GDPR may have on your organization?
CONTENTS

CHALLENGES 04
MATURITY OF PRIVACY REGULATIONS 05
CURRENT STATE OF PRIVACY 05
GENERAL DATA PROTECTION REGULATION 06
6 MAIN PRINCIPLES 07
CITIZEN’S RIGHTS 08
CONSEQUENCES OF NON-COMPLIANCE 09
GOVERNMENTAL SANCTIONS 09
PERFECTING PRIVACY 11
GAP ASSESSMENT 13
VALUE FOR ORGANIZATIONS 14
**Challenges**

With rapid technological advancements, many industries are digitally evolving and the businesses within are constantly changing their operations to maintain pace. Emerging and developing tools now allow businesses to gather and store heaps of consumer data, some of which not necessary.

Prior to any privacy directives, citizens were unaware of their data and its use. However, following various privacy and security breaches, citizens developed a growing concern for their data.

As a result, governmental directives were established to regulate businesses to ensure the privacy and protection of personal data.

"Prior to any privacy directives, citizens were unaware of their data and its use."
Maturity of Privacy Regulations

(2000) Safe Harbor
(2016) GDPR

Current State of Privacy

Although laws continue to evolve, new technologies constantly create additional privacy challenges putting personal data at risk, whether the information is sold, disclosed, or rented.

Due to the abundance of collected data and complexity of infrastructures, it can be difficult to detect misuses whether malicious or accidental. Privacy breaches can occur widespread in any industry or business regardless of the size, industry, or location. Some of the most recent and notable real-world examples are Uber and Samsung.

Uber, the international car-sharing taxi service company, developed a tool called, ‘God View’ which allowed the company to track Uber customers in real-time. The functionality, used as a method for sales enhancement, proved problematic as the individuals being tracked were identifiable due to their real-time location data.

Another incident earlier in the year was Samsung’s smart TVs. These electronic devices started collecting and recording user data, including activity and voice commands, and sending it to third-parties. As a result, Samsung now notifies customers and recommends switching the functionality off.

There are many controversies over certain business tactics, consumer privacy and appropriate data use, including tracking IP addresses for advertising use.
General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a regulation that is intended to strengthen and unify protection of personal data for European Union (EU) citizens. Created by the European Parliament, the Council of the European Union and the European Commission, the regulation is an addendum replacing existing data privacy laws and directives.

Through GDPR, the European Parliament focuses on giving control back to its citizens regarding their personal data and simplifying regulations for international businesses operating within the EU and exporting personal data globally.

These objectives are made possible through GDPR by:

- Combining existing data protection frameworks
- Creating guidance on best practices for privacy
- Expanding EU citizens’ control over their personal data

Early adoption for this regulation began in April 2016 and the mandatory compliance deadline was May 25, 2018. Those not compliant are subjected to harsh financial penalties.

Who’s Subjected to the Regulation?

GDPR applies to businesses inside or outside of the EU that collect and process any type of EU citizens’ personal data. More specifically businesses that operate as either a controller and/or a processor of personal data.

**Controllers**
Businesses that collect EU citizens’ data
- Pharmacists, general practitioners, tax authorities, financial institutions, etc.

**Processors**
Businesses that process data on behalf of controllers
- Payroll companies, accountants, market research companies, cloud service providers, call centers, etc.

In an aim to hold businesses, especially those outside of the EU, accountable for the use and protection of EU citizens’ data, any business with EU citizen customers is required to comply with GDPR.
6 Main Principles

Built around 6 specific privacy principles, GDPR creates fundamental requirements that businesses must follow during collecting, processing and managing processes. When handling personal data, the privacy principles are as followed:

1. Lawfulness, Fairness, and Transparency
Businesses must disclose and notify individuals of any data processing that will occur, and must follow processing procedures as described. Any personal data processing must comply with GDPR tests.

2. Legitimate Purpose
Businesses must only collect and obtain information for “specific, explicit and legitimate purposes.” That data can only be processed for which the individual was notified and consented.

3. Data Minimization
Personal information collected must only be the minimum amount needed for specific processing. Meaning, all personal information must be “adequate, relevant and limited” for necessity.

4. Accuracy
For the appropriate information, the data should be accurate and kept updated when known to be incorrect, if required.

5. Storage Restriction
Only using and storing personal information for sufficient processing or necessary purposes. Any other data is required to be removed from storage.

6. Integrity and Confidentiality
Businesses must properly protect personal data against unauthorized or unlawful processing, access, loss, or modification.

Personal Data

The main objective of GDPR is to enhance privacy and protection of personal data or Personally Identifiable Information (PII), which means any information relating to a person, either directly or indirectly, regarding their identity. Although a very broad scope, this information includes, but not

- Name
- Medical Records
- Photos
- IP Address
- Email
- Social Media
- Biometrics and Genetic Data
- Banking Information

Personally Identifiable Information (PII), which means any information relating to a person, either directly or indirectly, regarding their identity.
Citizens’ Rights
As part of the requirements, businesses looking or needing to comply with GDPR must identify and implement specific rights within their policies.

Policies must contain these mandated rights:
- Right to be informed when data is collected
- Right to object to data collection
- Right to access collected data
- Right to challenge and change data
- Right to transfer data easily between any processors
- Right to be forgotten (erase data)

By requiring these rights, GDPR can provide EU citizens control over their personal data by designing specific criteria for use based on the individual consent. Depending on the type of personal data, businesses will require two different types of consent.

1. Unambiguous Consent
Businesses will require unambiguous consent for non-sensitive information
- Social media, business telephone numbers, etc.

2. Explicit Consent
Businesses will require explicit consent for sensitive information
- Medical records, social security numbers, etc.

Demanding consent notifies and educates citizens of the use of their data and will facilitate accountability for better processing, transmitting, and management of data.
Consequences of Non-Compliance

Many businesses that are GDPR non-compliant and/or experience a privacy breach can face a myriad of consequences causing severe organizational damage.

Possible consequences include:

- Legal penalties
- Financial burdens
- Tainted reputation

Governmental Sanctions

Under GDPR, businesses (specifically controllers and processors), that violate and/or are not compliant are subjected to several legal sanctions enforced by EU government. For first case non-intentional non-compliance, businesses will receive a written warning. Most non-compliant businesses will undergo EU Commission-directed data protection audits. Some cases will result in restricted access to data as well as loss of organizational certifications. One of the biggest consequences are the financial costs relative to the breach and fines ranging from $11 – $22 million.

It goes without saying that the cost of non-compliance depends on the situation. By not abiding to GDPR policies including breach notification, conducting a PIA, and loss of records can result in a fine of 2% of annual turnover or approximately $11 million. For more serious infringements, such as lack of consent, disregarding individual rights, violation of core principles and data transfers to third-parties can result in fines of 4% of annual worldwide turnover in the financial year or approximately $22 million, whichever is greater.
EU TO FINE 4% FOR PRIVACY LOSSES

The European Union can fine corporations up to 4% of revenue for breaches of privacy. How U.S. corporations could be affected:

- **Apple**: $233.7 billion
- **Microsoft**: $93.6 billion
- **Alphabet (Google)**: $66.0 billion
- **Facebook**: $12.4 billion
  - **Fines**: $0.5 billion
  - **Revenue**: $2.6 billion

However, compliance is not just a matter of avoiding fines; citizens care deeply about the abuse and loss of their data resulting in a damaged reputation, which can be more costly than financial punishments.
Perfecting Privacy

To follow the established privacy principles and to respect the rights of individuals, there are several steps to comply with GDPR. Businesses should start by recognizing and understanding the specific policy requirements within the regulation.

<table>
<thead>
<tr>
<th>Key Policy Requirements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breach Notifications</td>
<td>Notify data subjects and supervisory authority within 72 hours of a breach</td>
</tr>
<tr>
<td>Consent</td>
<td>Justify processing personal data, and acknowledge consent</td>
</tr>
<tr>
<td>Accountability</td>
<td>Provide a letter that contains information explaining purpose of data</td>
</tr>
<tr>
<td>Privacy Notice</td>
<td>Comply with the regulation by deploying and demonstrating both policies and principles regarding the regulation</td>
</tr>
<tr>
<td>Territorial Scope</td>
<td>Process the personal information of EU citizens (in the EU) is applicable to the regulation</td>
</tr>
<tr>
<td>Security Obligations</td>
<td>Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services</td>
</tr>
<tr>
<td>Pseudonymisation</td>
<td>Encrypt all personal data and provide necessary security measures</td>
</tr>
<tr>
<td>Data Protection Officer</td>
<td>Hire personnel dedicated to monitoring GDPR compliance</td>
</tr>
<tr>
<td>Privacy by Design</td>
<td>Manage and minimize access to confidential data</td>
</tr>
</tbody>
</table>

By complying with these specific requirements, the EU can ensure that businesses provide two things: data protection, and responsibility and accountability.
Citizens’ Rights

**Stringent Data Protection**

By applying the requirements above, businesses must add encryption keys to all data. By encrypting data, businesses can limit the access and better monitor activity. Any activity that constitutes as a breach must be reported to the controller within 72 hours and to all individuals affected in a timely manner. Any data that is not necessary is required to be disposed of in approved sanitization methods. The Data Protection Officer (DPO) will be responsible for overseeing all data protection efforts and is responsible for maintaining GDPR compliance.

**Responsibility and Accountability**

Through GDPR compliance, businesses are held responsible and accountable for demonstrating commitment and achievement of personal data protection. To do so, by fulfilling the mandated requirements businesses will need to create and implement internal data protection policies as well as implementing built-in protection solutions for all processing activities. Through these new solutions, businesses can monitor all personal data for accuracy and malicious activity. Businesses will be required to conduct regular audits on the appropriate protection solutions as well as train personnel on requirements, policies, and new mechanisms.

“Data privacy is becoming a growing concern for end-users, and thus a push has been made for organizations to implement policies and procedures to ensure that data privacy is being protected,”

– Petar Besalev, Director of Cyber Risk and Privacy at A-LIGN

“A-LIGN can help organizations learn more about the importance of privacy, secure information appropriately, and implement the appropriate policies and procedures to ensure that end-users are confident that their data is secured. At the end of the day, our goal is to help organizations build stronger relationships with their clients by offering them that sense of security.”
**Gap Assessment**
As a way to calculate and understand the current level of compliance, businesses can undergo a gap assessment. This will review the business’ current data protection and privacy environment. The assessment provides a detailed report that summarizes compliance and evaluates overall readiness. This identifies any GDPR requirements not met allowing the business to remediate and comply.

**Validation**
If businesses are ready to comply fully, they can choose to get GDPR validated which tests compliance against the actual GDPR standard by reviewing policies, procedures, and processes in place. This ensures that the business will and can meet the requirements.

**Steps for Compliance**

1. Evaluate overall readiness
2. Discover risk areas within the business
3. Identify risk mitigation recommendations for improved security
4. Implement solutions within the business
Value for Organizations

Adhering to the regulation is much more than just avoiding legal and financial penalties associated with non-compliance. Becoming GDPR compliant presents a new opportunity for businesses along with a myriad of benefits. By demonstrating best practices and conformity, businesses will experience an increase in overall data security, improved brand reputation, and testimonial proof of security and privacy commitment.

For SpringCM customers, compliance with all national and international data regulations, including GDPR, is a top priority. This regulation establishes a whole new slate of responsibilities for how businesses deal with data to protect the privacy of users which creates an environment built around assurance and consumer trust.

“- Erik Severinghaus, Chief Strategy Officer & Head of Global Alliances at SpringCM

GDPR also impacts business operations, making them more efficient. The storage limitation requirements facilitate reduced storage costs. While security obligations, pseudonymisation, and DPO requirements will result in lower security risks and likelihood of regulatory intervention.

Through individual consent and privacy notices, businesses will encounter more timely customer interactions, resulting in more effective and useful data making less wasteful marketing campaigns.

Lastly through all the adequate controls, policies, and procedures which are compliant with GDPR, businesses instill Confidentiality, Integrity, and Availability values that enhances customer relationships through establishing trust.