GDPR 200 Course

Navigating GDPR

A Resource Developed by SIA Partners

secure|set

Agenda

1 section

The General Data Protection Regulation (GDPR)

- Introduction
- Understanding the scope of GDPR
- Focus on the key changes

2 section

What can we do?

3 section

Questions?

1 The General Data Protection Regulation (GDPR)

section

- ***Introduction*** ◀
- *Understanding the scope of GDPR*
- *Focus on the key changes*

GDPR by the numbers

A number of superlatives comes to mind

The General Data Protection Regulation (GDPR) is a strong data protection law. It gives customers more control over their data and includes new obligations for companies.

99 ARTICLES

56,000 WORDS

260 PAGES

During the committee stage at the European Parliament, almost

4,000

amendments were filed, a record for any EU regulation

It has taken

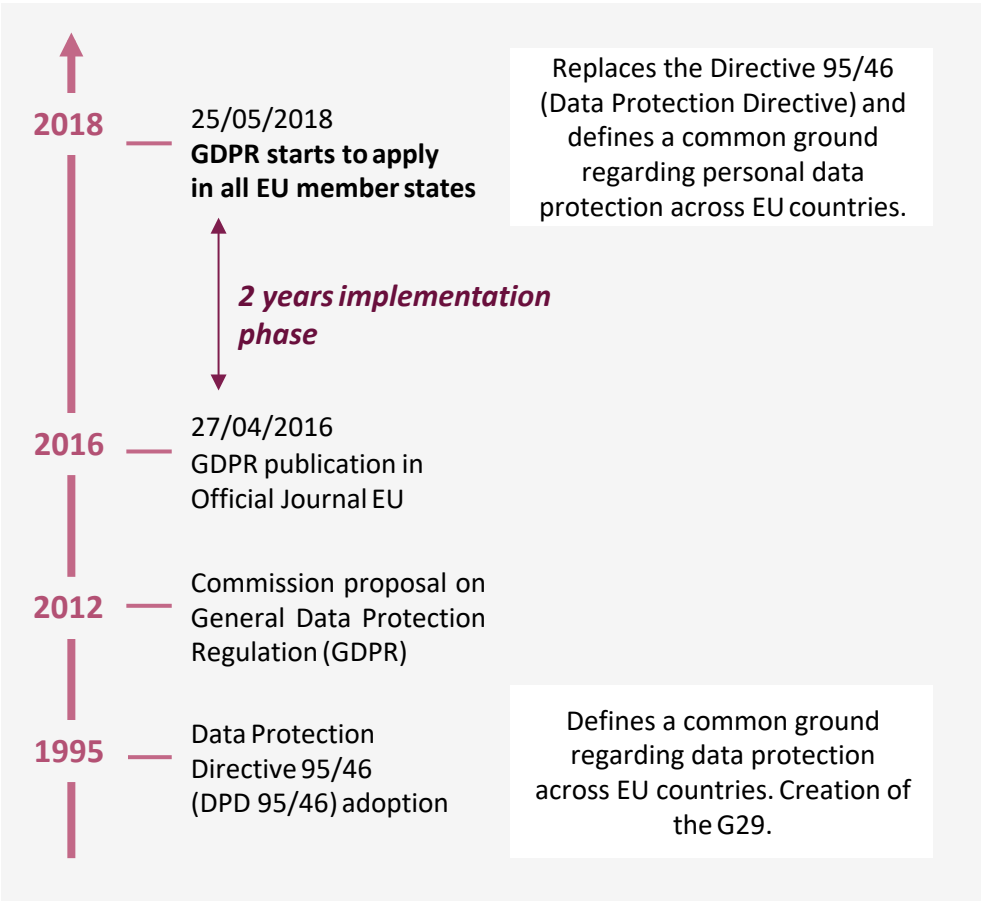
4.5

years of tough negotiations to reach agreement

Scope, Timeline and New Concepts

GDPR to take effect in May 2018

Timeline



GDPR is a regulation: it will be directly effective without the need for implementation legislation.

What's new under GDPR

- Wider scope on data regulation
- New obligations for data processor and controller
- New rights for data subjects/customers
- A new Accountability Principle makes controller responsible for demonstrating compliance with the data protection principles

Key data collection principles

GDPR built on existing Data Protection principles

- Lawfulness, Fairness and Transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality

Key Takeaways

- Think about GDPR Readiness as a large cross-functional program -> **Do not underestimate the size and scale**
- Build on your existing Privacy Program -> **Do not panic**
- Communicate to internal and external stakeholders -> **Be ready to educate your customers and employees**

New Rights and New Obligations

Substantial and Ambitious Change

Key GDPR Objectives	**Establish Data Privacy as a Fundamental Right** *GDPR considers data protection as a fundamental human right*	**Elaborate on the Data Protection Principles** *GDPR mandates companies to consider assessment and preventive/detective controls*	**Clarify the responsibilities for EU Data Protection** *GDPR applies to controller and processor*	**Increase Enforcement Powers** *EU aims to ensure compliance and impose fines for any non-compliance*
				
Major Impacts	**EU individual rights enhanced, harmonized and extended globally** ▪ Inform / Access / Rectify / Erase / Object ▪ Give or withdraw data specific content ▪ Transfer personal data to other providers	**Broadened Scope of Personal Data** ▪ "Employee, Customer, and Supplier Data" ▪ All direct and indirect identifiers ▪ Behavioral, self-identified and derived data	**Organizational Impacts** ▪ Stringent Data Security and breach notification ▪ Data controllers and data processors liable for breaches ▪ Appoint a mandatory Data Protection Officer ▪ Conditions for cross-border data transfers	**Increased cost of non-compliance** ▪ Fine of up to 4% of the preceding year's global revenues or 20 million Euro ▪ Data Privacy Authorities empowered ▪ Significant Reputational Risk

One of the most significant challenge is the global scope of the GDRP's application. Many companies will have to overhaul their data collection and data removal programs to become GDPR- compliant and avoid huge fines.

Establish Data Privacy as a Fundamental Right

US vs EU: Compare and Contrast

What do these two things have in common?

Both are protected by Constitutional (like) Rights

- **US Bill of Rights** (March 4th, 1789) – Freedom of Speech
- **EU Charter of Fundamental Rights (2000) -** Article 8(1): Everyone has a right to the protection of personal data

EU data protection law applies to personal data. Information that does not fall within the definition of "personal data" is not subject to EU data protection law.

Understanding Important Differences

	United States	European Union
Personal Information	Personally Identifiable Information (PII). Examples: Phone, number, address, name, Social Security Number	Personal Data – EU definition is broader; it includes information/data that can be used to ascertain the identity of the individual. Examples: phone number, address, name, social security number, dynamic IP addresses and unique online identifier.
Sensitive Data	Sensitive personal information – no specific list, depends on the context (incl. SSN, bank details)	Specific List: "*Data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data*." . Do not include Financial, SSN and child data.
Consent	Legitimizes many habits in the US	Strict requirements for a valid consent, i.e. freely given, specific and informed in the EU.
Data Breach	In most states, data breach is triggered only upon exposure of information that can lead to fraud or identity theft, such as financial account information.	Broader definition – A "personal data breach" is "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."
Data Transfer	No restriction on international data exports	General prohibition in the EU with exception (Privacy Shield Framework, etc.)
Retention	Often indefinite in the US	"No longer than what is necessary"

Elaborate on the Data Protection Principles

Protective Approach to Personal Data

Are IP addresses personal data?

What about unique device identifiers or biometric identifiers?

Does the data remain personal if you hash or encrypt it?

Personal data and unique identifiers

Personal data is defined as *"Any Information related to an identified or identifiable natural person"*	This includes both direct and indirect identification – e.g you know me by name – that is direct identification-; you describe me as "one consultant at your company working in New York" that is indirect identification
Identification can means "*an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*"	This has caused a lot of debate in the EU – Could an identification number includes an IP address, mobile device IDs or cookie string? And, the answer is yes.
Personal Data includes **Sensitive Data**. Enhanced protections and explicit consent is usually required where these data is processed	Biometric data (fingerprints, facial recognition, retinal scan etc.) and genetic data (gene sequence) are treated as sensitive data

Pseudonymous data

New GDPR concept: **pseudonymous data**, i.e. personal data subject to technological measures (hashing or encryption) such that is does no longer identifies an individual without the use of additional information	• Still considered as Personal Data • Less stringent data breach notification obligations (because no risk of harm), possible exemption for access/ erasure/ portability, and greater flexibility to conduct data profiling without consent

Increase Enforcement Powers

Administrative Fines, Remedies and Liabilities

Cost of non-compliance in the US

If you think compliance is expensive – try non-compliance

Fines up to **4% of revenue or €20M**, whichever is higher, for the most serious infringements (e.g. not having sufficient customer consent to process data), and 2% of revenue or €10M, whichever is higher, for the less serious breaches.

A list of points to consider when imposing fines (such as the nature, gravity, duration of the infringement and previous infringements) is included.

The **stakes are higher** and is gaining the attention of the **C-suite**

Different set of laws and enforcement practices

	United States	European Union
Data Protection	• No federal data privacy law • Sector-specific laws (healthcare, financial services) • Multiple state privacy laws • Unfair and Deceptive Practices enforcement by FTC	• Data Protection Directive/GDPR and E-Privacy Directive • National Implementation by each member state • Data Protection authority for each member state
Enforcement	• At a federal level – FTC enforcement • At a sectoral level – specific regulators (e.g. FCC) • At a state level – State Attorney General • At a consumer level – class actions	• At a pan European level – coordination • At a national level – National Data protection Authorities • At a sectoral level – specific regulators • At a consumer level – civil actions (rare)

1

section

The General Data Protection Regulation (GDPR)

- *Introduction*
- ***Understanding the scope of GDPR*** ◀
- *Focus on the key changes*

GDPR Extraterritorial Scope

The new rules will apply to many businesses in the US (1/2)

Highlights

- As a general rule, GDPR applies to the processing of personal data in the context of the activities of an entity established in the EU, whether or not the processing takes place in the EU.
- **In addition, GDPR will also apply to businesses located outside of the EU that offer goods and services, or monitor the behavior of individuals that are in the EU.**

Non-EU companies targeting or monitoring EU individuals

Offering of Goods and Services

× Accessibility of a site from within the EU, or contact addresses accessible from the EU is not sufficient

✓ Use of an EU language/currency, ability to place orders in an other language and references to EU users are relevant factors

Monitoring

✓ Tracking of individuals online to create profiles, including where this is used to take decisions to analyze/predict personal preferences, behaviors and attitudes

Wait… what if I don't have establishment within the EU?

- Where a controller or processor does not have an establishment within the EU, **it must designate a representative in the EU***.
- The representative will serve as a **point of contact for complaints** from data subjects and **deal with regulatory matters** in the EU in addition to or instead of the controller or processor that is located outside the EU.

**Unless the processing is occasional, does not include special "sensitive" categories of data, or data relating to criminal convictions and offenses*

Examples from all industries

- A US company offering goods and services to EU residents operating a global website from the US and obtaining Personal Data from clients
- A US-based hotel chain or airline company that stores information of EU individuals travelling to the US
- A mobile application that monitors the behavior of EU visitors through code that allows the collection of data intended to be used for interest-based advertising
- A supplier based on the US with no "establishment" in the EU and none of its servers located in the EU, offering cloud computing services to individuals who reside in the EU

It is not clear if non EU companies offering goods and services to EU businesses (≠ individuals) will be deemed in scope.

GDPR Extraterritorial Scope

The new rules will apply to many businesses in the US (2/2)

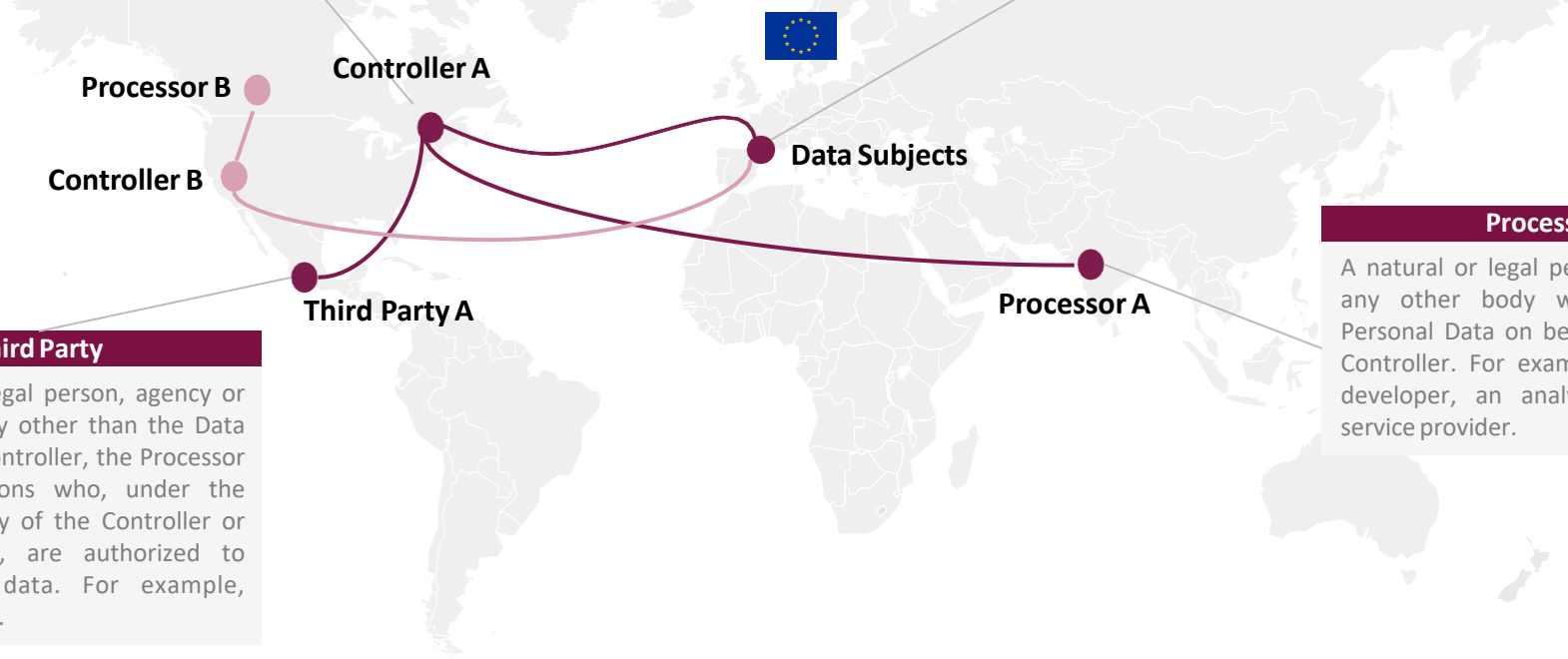
THE IMPACT ON CANADIAN COMPANIES IS MAINLY BASED ON THE VARIOUS ACTORS AND THEIR ASSOCIATED ROLES

Controller

A natural or legal person, public authority, agency or any other body which determines the purposes and means of the processing of Personal Data. For example, a controller can be an organization.

Data Subject

A person who can be identified directly or indirectly by means of **identifier**. For example, an identifier can be an national identifier, a credit card number, a username, or a web cookie.



Processor

A natural or legal person, agency or any other body which processes Personal Data on behalf of the Data Controller. For example, a tester, a developer, an analyst or a cloud service provider.

Third Party

A natural or legal person, agency or any other body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the data. For example, subcontractors.

THE CONTROLLER AND PROCESSOR ARE LOCATED OUTSIDE THE EU, BUT IS STILL SUBJECT TO GDPR

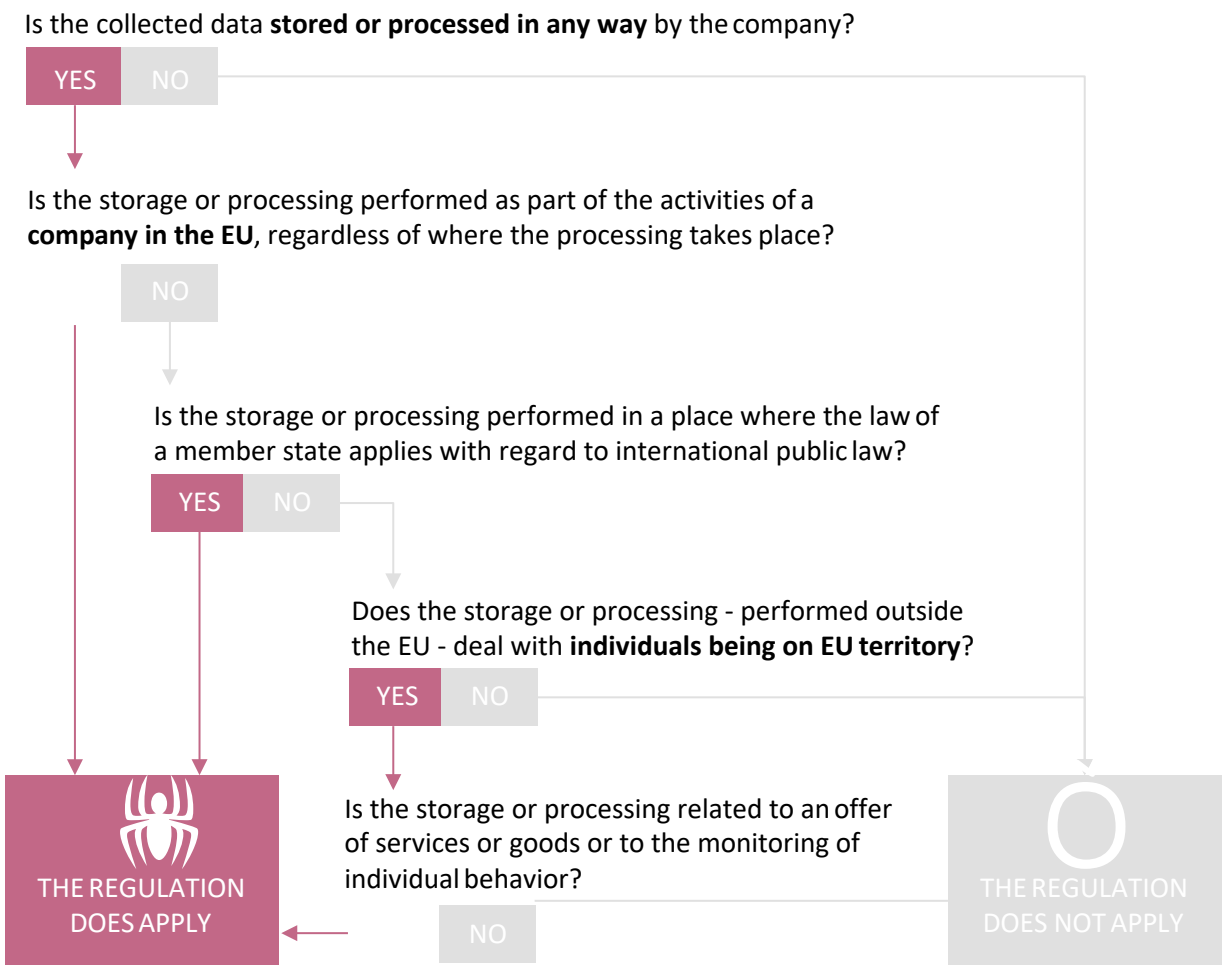
Note: PIPEDA has limited application to processors of data

GDPR Extraterritorial Effects

In synthesis: **Am I impacted?**

A SIMPLE DIAGRAM FOR YOUR MOST CRICTICAL QUESTION

The application scope of the regulation is quite broad.
In particular, it encompasses a rule setting out the extra-territorial application of EU law and subcontractors are directly in scope.



EXAMPLES FOR (RE)INSURANCE COMPANIES

✓ Manipulating information about a life / health insurance policyholder living in Europe

Ò Manipulating information about a life / health insurance policyholder living in the US

Most common misconceptions under GDPR

The scope of application for data protection is widening

MISCONCEPTION		ANSWER & ANALYSIS
The GDPR is only about **online data**	NO	The GDPR is **technology neutral**. Thus, the new rules apply to personal data both in the online and offline world (e.g. paper filing system).
I am only processing B2B data, so the GDPR is not for me	NO	The GDPR applies to the **processing of personal data**, and **does not differentiate** between personal data from the B2B and the B2C world. Personal data in the B2B world includes work email address, work direct dial number, name, job title, and workplace postal address because this data identifies a living individual.
I don't process data automatically, the GDPR is not for me	NO	The GDPR applies to personal data which are processed **automatically** (e.g. profiling), **partially automatically**, or processed by **any other means**, including manual processes (i.e. by a human being).
I only need to review my privacy policies and privacy notices to comply with the GDPR	NO	The GDPR **increases the standards** of already existing obligations related to data protection (e.g. consent has to be given unambiguously and organizations will have to provide more information to individuals about their data processing activities).
I have the consent of individuals to use their data, I don't need to implement the GDPR	NO	The GDPR increases the standards for data protection, including the requirement that consent of an individual to data processing activities must be **unambiguous**. Consent cannot be implied from inaction but must be the **result of a positive action** by the individual. Consequently, marketers will have to review how they collect consent from individuals to receive communications. However, the GDPR also recognizes alternative legal grounds for processing personal data.
I can use a global data source for **all my business areas**	Partially NO	Data sources from one area of the business cannot be used to analyze claims unless the **documentation wording, agreed by the customer**, is sufficient to allow firms to use data collected in another area of the organization for insurance pricing.

Personal Data

Data Processing Methods

Consumer Protection

Industry Standards

The **definition of these key concepts** is becoming broader, thus enlarging the scope of application of the GDPR

GDPR extraterritorial scope

Don’t underestimate the influence on local regulators…

Last but not least, over the past few years the industry has witnessed that US regulators have a tendency to leverage EU regulations / regulatory projects to refine the local frameworks

According to Sia Partners, they foresee that the implementation of GDPR in Europe is likely to trigger some local regulatory adjustments to enhance data security locally and to foster consistency of the frameworks between the US and Europe.

1 The General Data Protection Regulation (GDPR)

section

- *Introduction*
- Understanding the scope of GDPR
- ***Focus on the key changes*** ◀

Focus on the key changes

Table of contents

This section will provide you with an overview of the key changes brought by GDPR

Focus on the key changes

Impacts synthesis and how to read them

Here is defined 4 axis operational impacts to foresee the stakeholders involved and the relative workload corresponding to a GDPR remediation plan. Below is an overall summary of these impacts.

Governance

This regulation encourages companies to implement a self-sufficient data protection framework. One of the key challenges will be to secure a regular communication across all departments and the Data Protection Officer. Implementing such framework require animating a network of correspondents to ensure communication effectiveness.

Information systems

One of the rationales for this regulation was to take technological evolutions into account. Beyond the enhancement of data security practices, companies will have to implement features to be able to track data to identify potential breaches, to oversee the respect of data retention periods, and to enable data deletion. On the other hand, companies will have to secure an appropriate level of protection since the design of new tools / applications (Privacy by design) processing personal data.

Reporting

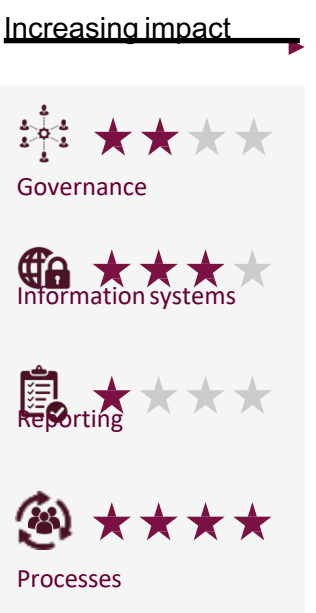
Insurers will also have to implement new production processes for reporting to the customers (what data is collected and processed), to the regulatory bodies (data breaches, processing inventory) and executives (privacy impact assessments, report on the data protection framework annual review)

Processes

Companies will have to adapt the way they collect personal data. The introduction of explicit consent, the privacy by design & by default and the right to be forgotten, make it mandatory for companies to clarify the kind of data necessary to their activities and to continuously answer client requests, including request for a transfer to a competitor (data portability). Auditing and adapting the existing processes will be inescapable.

Alignment Index

For the following pages, we will evaluate the changes' impacts according to these 4 axis, as illustrated below:



Lawfulness of Processing and Consent

Conditions for legal data processing and consent

Lawful Basis for Processing Personal Data

The processing of personal data of EU data subjects is unlawful unless an exception applies. The lawful grounds are broadly similar to those in the Data Protection Directive, including:

- the processing is **necessary** for certain defined activities (e.g. compliance with a legal obligation to which the controller is subject, for purposes of the legitimate interests pursued by the data controller or for the performance of a contract); and/or
- the data subject has given **consent** to the processing of the personal data for specified purposes.

Conditions for a Valid Consent

GDPR has a **wider definition:** the consent of the client must be "*freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement of by a clear affirmative action, signifies agreement to the procession of personal data relating to him or her*"

For a valid consent, you need to ensure:

- Consent is active, and does not rely on silence, inactivity of pre-ticked boxes
- Consent is not bundled with other written agreement
- Supply of services is not conditional on consent to processing
- Clients are informed about the methods for withdrawing consent (including the same medium used to obtain consent)
- Separate consent are obtained for distinct processing operations

IMPLICATIONS

- **Understand what** personal data you capture and become more careful about **what you collect.** You need to collect the minimum set of personal data to achieve your business goal
- **Review the grounds for lawful processing** and check these grounds are applicable under GDPR
- **Consider the procedures and wording** used when obtaining consent from individuals
- Where relying on consent, make sure the consent **meets new requirements**
- Consent request must be **distinguishable, intelligible, easily accessible, revocable** and in clear and plain language in order to be valid

Key takeaways

- There are significant difference between the conditions for legal consent under the GDPR and US websites practices and habits
- Informed consent forms currently used are unlikely to be adequate to comply with the consent requirements of the GDPR

New Data Controllers' Obligations

Access, rectification and portability

Right of information and Access*

Data controllers must, **on request** and with **no fee**:

- Provide a copy of the data
- Confirm if personal data is processed
- Provide supporting and detailed explanations (e.g. retention period, criteria used to determine this period, details of disclosure to recipients in third countries).

The objective of access requests is to allow individuals to confirm the accuracy of data and allow them to exercise rights of correction, objection etc.

Right of Rectification and Portability*

- Individuals can have their personal data be ported to them, or be transmitted to another controller, in a structured, commonly used and machine readable format.
- Portability is narrower than access right because it only applies to personal data which is processed by automated means, directly provided to the controller or when the basis for processing is consent.
- Individuals can require a controller to rectify inaccuracies.

**There are exceptions where these rights would adversely affect intellectual Property Rights or Trade Secrets*

IMPLICATIONS

Companies must:

- **Review processes**, procedures and training to ensure they are sufficient to deal with the GDPR's Access and Portability Rules
- **Develop template** response letter to clients
- **Conduct an assessment** and develop an approach to provide data in compliance with the new format obligations
- **Consider developing client's access portals** to allow a direct exercise of these rights and **manage an increasing number of requests**

Key takeaways

- Align Processes and Policies to handle increasing requests
- Make sure people are trained to respond efficiently and accurately
- Make sure you have the rights tools in place

New Data Controllers' Obligations

Right to be Forgotten and Object

Extensive Right to be Forgotten (=erasure)

A new right is introduced

- A right to be forgotten (so-called "erasure") and for processing to be restricted

A new obligation for Data Controller:

- Clients will have a right to obtain the erasure of his/her personal data from the controller
- When the controller has made personal data public, she needs to take "reasonable steps, including technical measures, to inform the controllers which are processing the data" to obtain complete erasure

Right to Object to the processing of personal data.

- Only the right to object to direct marketing is absolute as there is no need to demonstrate ground for objecting and there is no exemption to allow processing to continue
- Right to object to processing based on legitimate interest, or processing for research or statistical purposed is not absolute
- Online services must offer an automated method of objecting
- Clients must be notify of these rights at an early stage

IMPLICATIONS

- Audit review processes to make sure **data deletion requests** are recognized and dealt with by employee and suppliers
- Determine if systems are capable of meeting the requirements to mark data as restricted (if erasure is not achievable)
- **Audit data protection notices** and policies to ensure that individuals are told about their right to object, clearly and separately, at the point of "first communication"
- **Review processes t**o ensure they are capable of operating in compliance with GDPR
- For online services, make sure, you have an automated way for this to be implemented

Key takeaways

- Right to be forgotten is not an absolute right. Look at the GDPR balancing requirements and put in place the right processes to handle requests
- The devil is in the details, especially if you have complex IT environment (e.g. you replicate data)

Data Breach Notification and Security

Finding the Right Balance

In the US, most companies dealing with customers already have a mature breach response program, either driven by security or legal requirements. However, during discovery of an incident, there is always a balance between getting all the facts and providing prompt notice. GDPR, and it specific requirements, may require a review and an update of your program, policies and procedures.

Data Breach Notification and Breach Register

- Data controllers and processors are now subject to a general personal data breach notification regime, e.g. 72 hour data breach notification requirement
- There is an obligation for the data controller to document each incident "compromising the facts relating to the personal data breach, its effects and the remedial action taken".

More Guidance on Data Security Standards

Security actions considered "appropriate to the risk" includes:

- The pseudonymisation and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures

IMPLICATIONS

- Implement **data breach response plan,** incident detection mechanism and **escalation**
- **Adopts** specific **breach notification guidelines**
- **Ensure level of security** is appropriate to the risk. For example, adhere to an approved code of conduct or an approved certification mechanism can demonstrate compliance with the GDPR's security standards.

Non-compliance can lead to a fine up to €10,000,000 or up to 2% of the total global revenue, whichever is greater

Key takeaways

- Review and update your Incident Identification Systems and Incident Response Plans
- Implement policies, procedure and related controls to review and test these procedures

Data Governance Obligations

Understanding Accountability Measures

GDPR requires the implementation of Accountability Measures to reduce the risk of breaches and to signify their commitment to data governance. Companies must design an develop Privacy Impact Assessment (PIA), audits, policy reviews, activity records and (potentially) appoint a Data Protection Officer (DPO).

Data protection by design and by default

Introduction of new data protection concepts

- **Privacy By design**: implement appropriate technical and organizational measures to protect the rights of the data subject and ensure compliance with the GDPR
- **Data Protection By default**: implement appropriate technical and organizational measures to ensure that only the minimized personal data that is necessary for a specific purpose is processed

- Introduce policies and procedures to ensure that appropriate measures and safeguards are incorporated when introducing new personal data processing systems, products or processes and to ensure that data protection by design and default principles are respected

Privacy Impact Assessments

Stricter impact assessment

- PIA are required prior to processing activities with "high risk for the rights and freedom of individuals"
- Including where personal data processing involves large scale processing of certain sensitive personal data, including genetic data and data concerning health

- Extra compliance step for new projects
- Budgeting in terms of time and costs
- CIO guidance for Privacy PIA requiring issues

Data Protection Officer

DPO appointment obligation under certain requirements (i.e. organizations engaging in large scale systematic monitoring or processing of sensitive personal data)

- DPO must be independent from processor and controller
- DPO functions as an internal regulator and a point of contact for customers and for the applicable supervisory authority
- DPO reports directly to highest management

- Analyze whether a DPO is required
- Review of current job specifications under GDPR
- Determine if multiple DPO appointment to cover different jurisdictions is required
- CPO and DPO can, but do not have to be the same person
- Review CPO's reporting line optimal

Key takeaways

- Staff training – consider mandatory training and interactive Q&A
- Impact analyses on all activities with personal data input/processing/output
- Overall audit on personal data possession and use required

Transfer of Personal Data

Restrictions on transfer of personal data from the EU

Companies that want to transfer personal data outside of the EU must assess whether the country ensures an adequate level of protection for individuals. Some countries are deemed adequate by virtue of a decision of the European Commission. While the US in not in this list, the EU decided that the transfer would be adequate so long as the company receiving data is part of an agreement know as the Privacy Shield (formerly Safe Harbor Framework).

- GDPR provide more detail on the particular procedures and criteria that the Commission should consider when determining adequacy
- Other existing methods of transferring data continue to be recognized: binding corporate rules or standard contractual clauses
- Transfers will be permitted when an approved code of conduct or an approved certification mechanism is used
- There a numbers of derogations in limited circumstances (consent, legitimate interests, legal claims)

IMPLICATIONS

- Review and **map key international data flows**
- Consider what data **transfer mechanisms** are in place
- **Review contracts with suppliers**
- Evaluate relationships with service providers and customers to establish a new legal basis for transfers

Key takeaways

- Consider the Privacy Shield as an additional step toward GDPR
- Breach of the GDPR's data transfer provision is one of the issues for which the maximum level of fines can be imposed (up to 4%, or annual revenue, or 20 million euros, whichever is greater)
- Non-compliance proceedings can be brought against controllers and/or processors

EU-US Privacy Shield

The future of transatlantic data transfers

Highlights

- In July 2016, the European Commission formally adopted the data transfer framework replacing the Safe Harbor Framework (invalidated in October 2015 in the case of *Schrems v. Data Protection Commissioner*).
- Participating in Privacy Shield in voluntary for companies regulated by the US Federal Trade Commission (FTC) or the US Department of Transportation (DOT).
- Transition for self-certification under Privacy Shield will demand higher budgets and burdensome data privacy obligations.
- In September 2017, the EU Commission will issue a critical assessment of whether Privacy Shield delivers what it should deliver.

	Update Privacy Policies and Procedures	Accountability on Onward Transfer of Personal Data	Robust Security Controls
Key Principles	• Privacy policies must disclose the purpose for which data is collected and used • Companies must provide notice to EU citizens on how data is collected and processed • Individuals must be provided with the choice to "opt-out" when their personal data is to be disclosed to a third party or to be used for a purpose "materially different"	• Companies transferring data must enter into a contract with the third party data controller • Data must only be processed for limited and specified purposes consistent with individual consent • Third Party must guarantee the same level of protection as Privacy Shield Companies	• Companies must take reasonable and appropriate measures to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction • Companies must retain data only for so long as it serves the purpose for which it was intended and must limit data retention provisions.
Main Tasks	• Assess the maturity of Data Compliance Mechanisms • Review privacy practices and ensure they align with the privacy policy • Develop and maintain a Privacy Policy based on Privacy Shield Principles • Produce a Gap Assessment Report	• Mapping Data Flows • Identification of Services Providers • Address onward transfers by reviewing and revising existing contractors for third-party vendors and onward transferees • Assess the Maturity of the Data Privacy Program	• Validate Security Safeguards with a customized security questionnaire deployed to system, application and interface owners • Update training for employees who have access to EU citizen Data

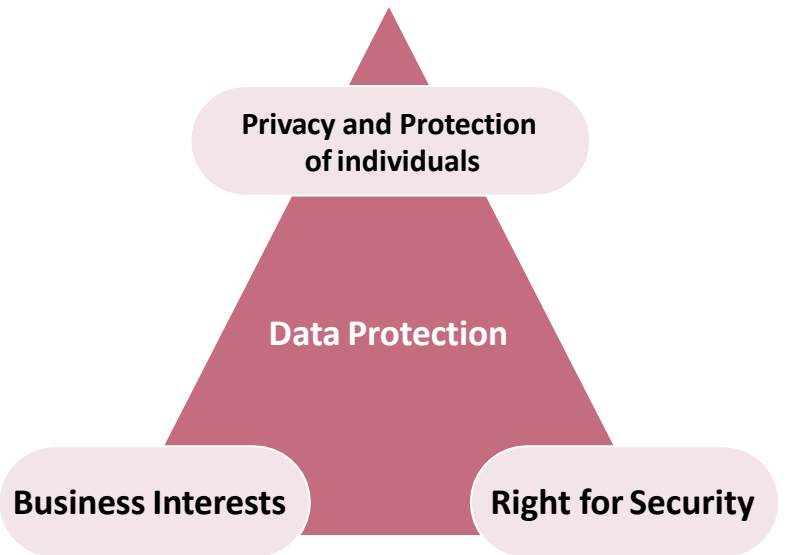
Why GDPR matters

Consider micro and macro impacts

Potential impacts on your company

1. IT / Security capabilities are required (cost and prioritization related issues)
2. Restrictions on transfer of personal data from the EU unless compliant with GDPR
3. Non compliance is subject to individual lawsuit in EU
4. Investigations are disruptive to business
5. Adverse Media and Reputational Damage

Data Protection Dilemma



Enforcement: one-stop-shop principle

- Regulated by the Data Protection Authority (DPA) in the Member State of "main establishment"
- This 'lead regulator' is responsible for supervising and enforcing all data protection complaints in any EU jurisdiction in which the entity operates

Key takeaways

You should understand the impacts of GDPR and determine an approach for Compliance taking into account where you are going strategically as a business and how data influences that, positively and negatively.

2 What can we do?

section

THE CORRECT APPROACH

Understand your exposure to personal and sensitive data

DATA PROTECTION CONCERNS EVERY BUSINESS

Your employees

- Business Functions
- Support functions

Use

- Applications
- End User Computing *(shared files, etc.)*

That contains

Data

- *Employees data*
- *Customers data*
- *Medical / personal data*
- *Etc.*

Stored in

Data Centers

- *GDC (HP)*
- *Local DC*
- *Cloud*
- *Etc.*

Need for data inventory

Data Usages	User Location	Data Source Location	Data Flow
Data Classification	Data Security	Data Location	

Challenges for Data Location & Security

Data stored in different places under different legislations. Would it be concerning security or transfers issues, the stakes and duties are numerous for any US organization.

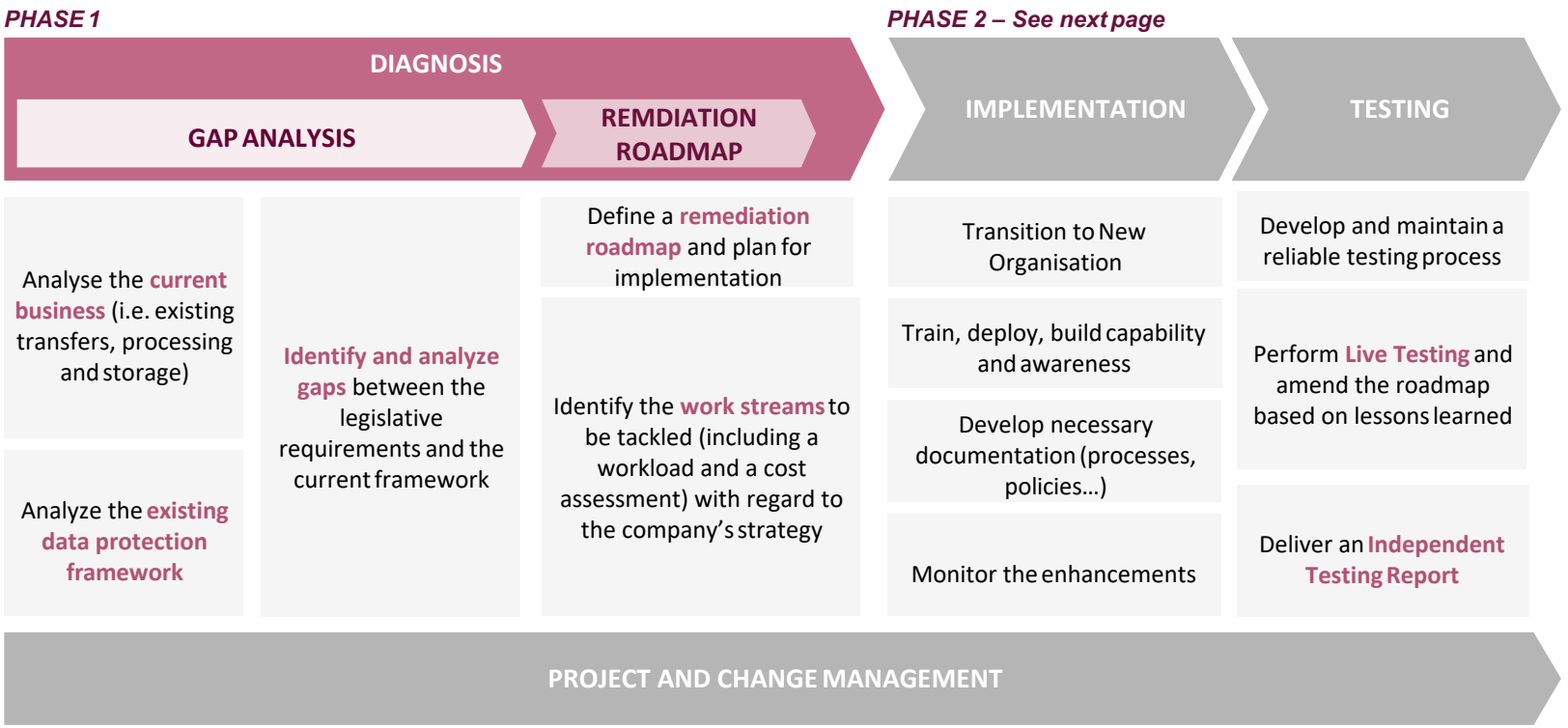
Requirements concerning client / regulatory compliance

To address the invasive regulatory environment, organizations must ensure they have appropriate resources in terms of Compliance network and processes

"THE CORRECT APPROACH IS TO PERFORM A DIAGNOSIS OF THE MATURITY LEVEL OF YOUR CURRENT FRAMEWORK "

THE APPROACH

PHASE 1 – DIAGNOSIS | The diagnosis approach for GDPR transformation



- *Directory of the processes impacted*
- *Data flow mappings and risk mapping*
- *Qualitative analysis of the maturity level*

- *Detailed action plan*
- *Mapping of the key procedures and controls*

- *Documentary basis*
- *Adjusted framework*
- *Material to raise awareness and provide training*
- *Deployment monitoring*

" ALL ALONG THE DIAGNOSIS, FOSTER THE STAKEHOLDERS' AWARENESS ROUND DATA PROTECTION IN ORDER TO BEST PREPARE FOR THE CHANGE MANAGEMENT "

THE APPROACH

PHASE 2 – IMPLEMENTATION | 4 key initiatives to conduct

TRAIN, DEPLOY, BUILD CAPABILITY & AWARENESS

Design information campaigns / training to foster understanding and reduce risks

- Training will help every stakeholder to **understand his / her responsibilities** within the new framework
- Moreover, a fair share of Data Privacy breaches are a result of **employees mistakes** (such as emails or fax sent to the wrong recipient, the loss of printed documents, information stored on the wrong server…)
- Thus, it is important to provide robust training:
  - ✓ Awareness campaigns for all employees (e.g. e-learning)
  - ✓ Advanced training for the employees dealing with personal or sensitive data

BUILD THE NECESSARY DOCUMENTATION (PROCESSES, POLICIES…)

Define and build data policies and operational procedures

- All the processes exposed to Data Protection risks must **document according to GDPR requirements**
- Controls must design according to the risks identified

MONITOR THE ENHANCEMENTS

Enhancing Data protection framework is an iterative process.

- Put in place controls and appropriate metrics

TRANSITION TO THE NEW FRAMEWORK

Manage the transition by helping operational stakeholders to take new framework into account in their daily activities

- Implementing a Data Protection framework requires **strong support for the operations and business teams** to play along with it. E.g.:
  - ✓ Effective deletion of some documents at the expiry date by the appropriate team
  - ✓ Each document containing personal data must be sent using an encrypted format

The appropriate philosophy

Launch a project adapted to your needs and capabilities

Start with the right questions

1 Where is stored personal and sensitive data that you collect? What is the **purpose** of their collection?

2 Have you already implemented a **data protection framework**? (roles and responsibilities, data protection policy, controls, annual report on the framework maturity and the definition of an enhancement plan…). If not, which department will lead the project?

3 What is your **maturity level** with regard to the current regulation?

4 What is your **strategy when it comes to using / leveraging data**? (Minimum collection to perform current activities vs. broad collection to explore potential opportunities)

Potential Implementation Challenges

- Develop the framework:
  - Encourage **employee's adherence** to the framework
  - Provide the Data Privacy Officer with means to **develop the framework**
- The **Information Systems ability** to match regulatory requirements (e.g. right to be forgotten)
- The collection of information from **subcontractors**
- The requirements in terms of **documentation** and its ongoing update

Key Success Factors

- Precisely assessing the **scope** of data and processes impacted
- Identifying the link between regulatory requirements regarding data protection and the **strategy of the company**
- Considering **framework sustainability** from its design to completion
- Encourage a **data protection culture** across internal teams

This is an opportunity to build customer trust and demonstrate your Privacy Program Maturity and GDPR Readiness

3

section

Questions?

Credits for the Presentation come from Sia Partners and are protected under copy write laws.

siapartners

https://sia-partners.com/