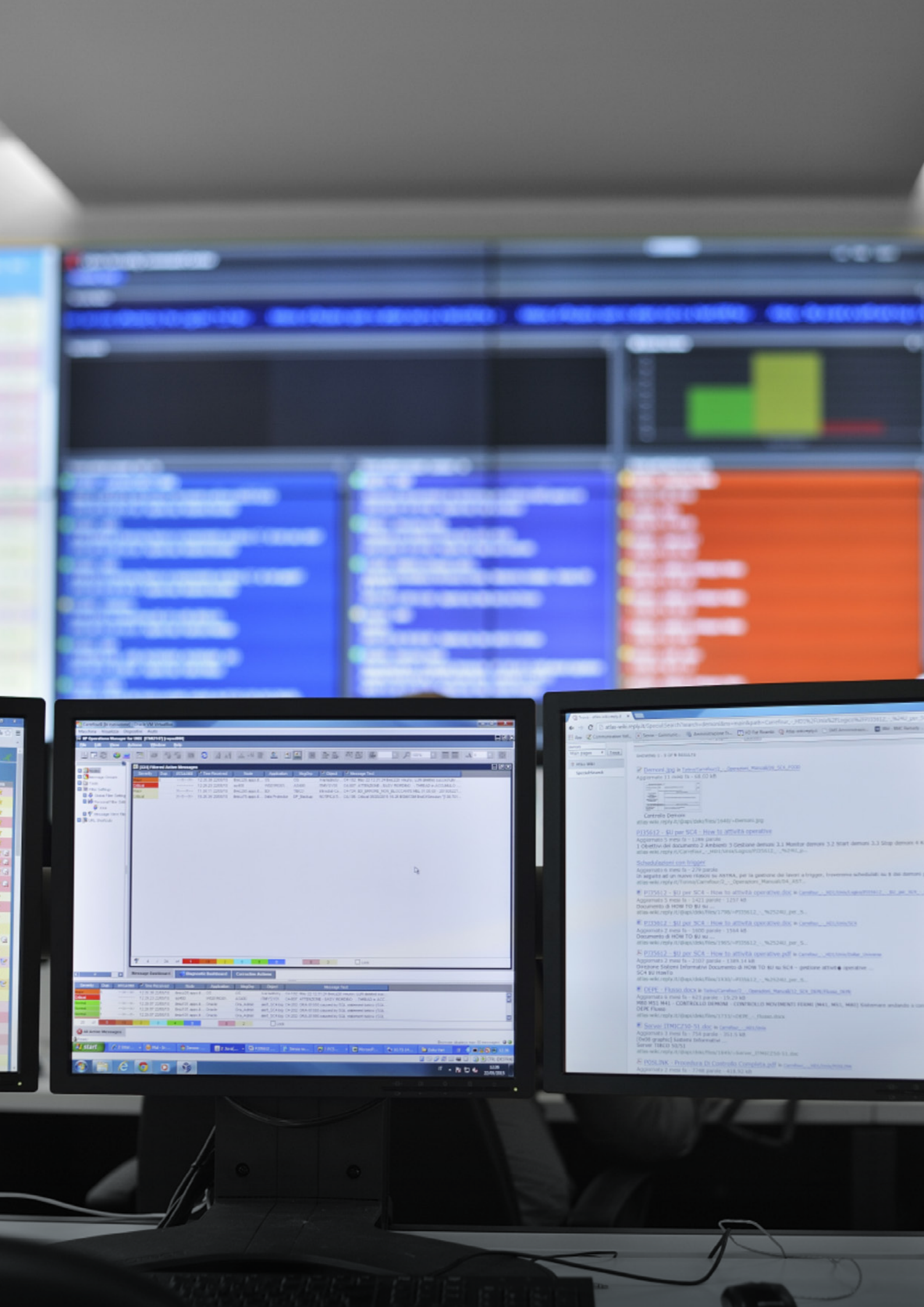


# GENERAL DATA PROTECTION REGULATION

**A REPLY PATH TO COMPLIANCE**

European companies are moving towards a new era of personal data protection. How to build an effective GDPR plan, which aims not to just be compliant but be an advantageous program?

Reply outlines an approach aimed at fostering a sound implementation of a data protection management system, that maximizes the value of GDPR as an opportunity to enhance data governance and to build customers' trust.



Windows 7 desktop environment showing a Microsoft Word document titled "P014/Personal Action Messages". The document content includes a table with columns for "Date", "Time", "Location", "Status", and "Message Text". The table lists several entries, including "12.28.2017", "12.28.2017", "12.28.2017", and "12.28.2017". The document is open in a window titled "P014/Personal Action Messages". The Windows taskbar at the bottom shows the Start button, a search bar, and several pinned applications including Internet Explorer, Google Chrome, and Microsoft Word. The system tray on the right shows the date and time as "2017.12.28".

Windows 7 desktop environment showing a Microsoft Word document titled "P014/Personal Action Messages". The document content includes a table with columns for "Date", "Time", "Location", "Status", and "Message Text". The table lists several entries, including "12.28.2017", "12.28.2017", "12.28.2017", and "12.28.2017". The document is open in a window titled "P014/Personal Action Messages". The Windows taskbar at the bottom shows the Start button, a search bar, and several pinned applications including Internet Explorer, Google Chrome, and Microsoft Word. The system tray on the right shows the date and time as "2017.12.28".

# THE NEW GENERAL DATA PROTECTION REGULATION

PRIVACY PERCEPTION IS GOING TO CHANGE SIGNIFICANTLY IN EUROPE OVER THE NEXT MONTHS BUT THERE IS STILL LITTLE AWARENESS ABOUT THE IMPORTANCE OF SUCH CHANGE, DESPITE THE HUGE MARKETING HYPE WE ARE EXPERIENCING SINCE THE EUROPEAN GENERAL DATA PROTECTION REGULATION (GDPR) PUBLICATION IN THE OFFICIAL JOURNAL OF THE EU.

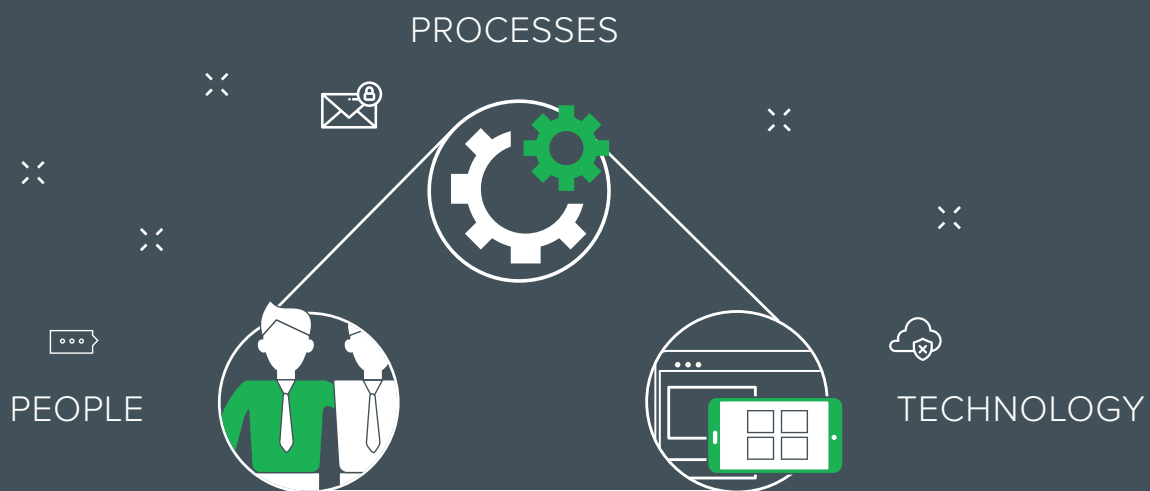
THE GDPR WILL BE DIRECTLY APPLICABLE IN ALL MEMBER STATES, WILL BE ADOPTED IN THE EUROPEAN ECONOMIC AREA AND WILL REPLACE THE EXISTING NATIONAL LAW IMPLEMENTATIONS OF THE DIRECTIVE 95/46/EC.

**THIS NEW DATA PROTECTION REGIME IS GOING TO BE APPLIED, STARTING FROM MAY 25TH 2018, IMPOSING STRICT ACCOUNTABILITY AND HIGH FINES (AS NEVER HEARD OF BEFORE IN CASE OF PRIVACY VIOLATIONS), HAVING AS MAXIMUM THE HIGHEST BETWEEN €20 MILLION AND THE 4% OF THE GLOBAL TURNOVER OF THE PREVIOUS YEAR.**

## GETTING READY IS NOT A “ONE-OFF” PROJECT!

The GDPR introduces the concept of “accountability” of the Controller for the processing of the personal data, that requires the capability to demonstrate compliance with the regulation and therefore the adoption of security measures defined on a “risk-based approach” in relation to the rights and freedoms of the Data Subject.

A complete GDPR Program to remediate any compliance gap should encompass three components:





The number and complexity of regulation requirements urge the development of a program of initiatives, aimed at identifying and implementing the different organizational and technical controls in time, balancing time and budget.



## KEY ELEMENTS

GDPR AIMS AT PROTECTING PERSONAL DATA OF EU CITIZENS, LIKEWISE THE 1995 DIRECTIVE. HOWEVER, DUE TO THE BREAKTHROUGH IN THE TECHNOLOGY LANDSCAPE OVER THE LAST TWO DECADES IT BECAME NECESSARY TO ADOPT A NEW APPROACH TO PROTECT PERSONAL DATA.

### RISK BASED APPROACH & ACCOUNTABILITY

IMPACTED TOPICS			
	<b>DATA PROTECTION OFFICER</b>	A Data Protection Officer (DPO) MUST inform, advise and monitor the organisation's compliance with the GDPR.	<b>ROLES AND RESPONSIBILITIES</b>
	<b>RECORDS OF PROCESSING ACTIVITIES</b>	Organisations MUST maintain internal records of processing activities, especially for high risk processing, such as special categories of data.	<b>DATA GOVERNANCE</b>
	<b>DATA PROTECTION IMPACT ASSESSMENT</b>	A DPIA tool SHOULD be used to assess the processing operations and their purpose, while evaluating all the measures in place to address risk.	<b>RISK MANAGEMENT</b>
	<b>RISK-BASED APPROPRIATE SECURITY MEASURES</b>	Security measures MUST take into consideration the risks relating to data, including the nature and purpose of its processing.	<b>RISK MANAGEMENT/ SECURITY PLAN</b>
	<b>DATA PROTECTION BY DEFAULT AND BY DESIGN</b>	Organisations must be able to demonstrate that data processing activities consider and enact data protection principles.	<b>CHANGE MANAGEMENT/ RISK MANAGEMENT</b>
	<b>EXPLICIT CONSENT AND LAWFULNESS OF PROCESSING</b>	Before processing personal data, the Data Subject must give provable consent to the processing or the given requirements for lawfulness of processing must be met.	<b>DATA GOVERNANCE</b>
	<b>EXPANDED TERRITORIAL REACH</b>	The GDPR applies to data processing of EU residents, irrespective of whether that data processing is carried out inside or outside EU borders.	<b>CONTRACTUAL CLAUSES</b>
	<b>DATA PORTABILITY &amp; RIGHT TO BE FORGOTTEN</b>	Procedures MUST be defined to manage requests from individuals wishing to transfer their personal data to another provider, and wishing to delete personal data no longer in use.	<b>DATA GOVERNANCE</b>
	<b>DATA BREACH</b>	Organisations MUST have data breach procedures that notify the supervisory authority within 72 hours of becoming aware of the incident, and/or notify the Data Subject without undue delay.	<b>INCIDENT MANAGEMENT / LOG MANAGEMENT</b>

# THE REPLY APPROACH

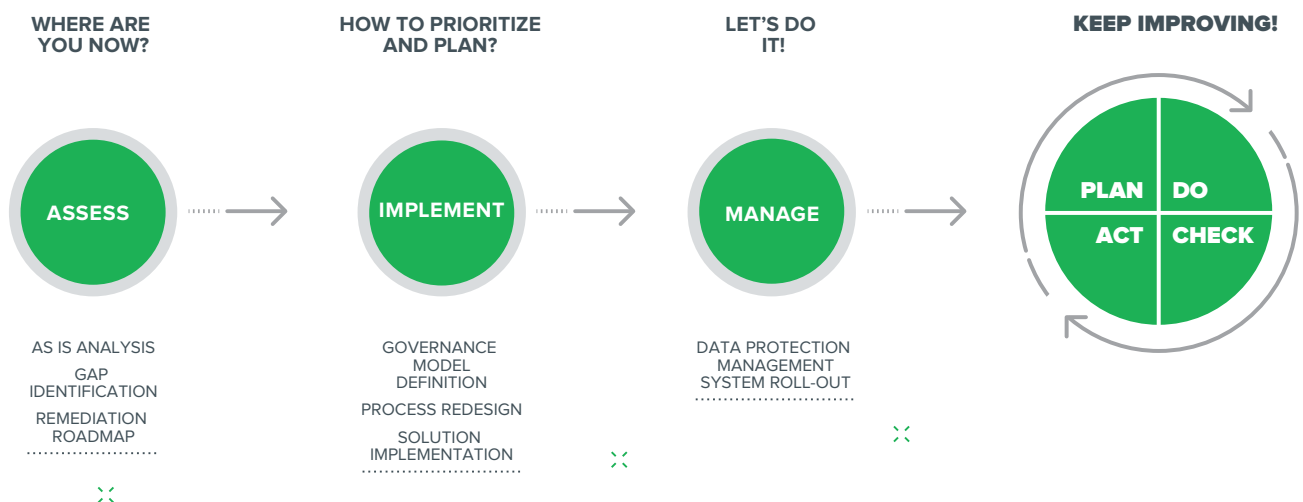
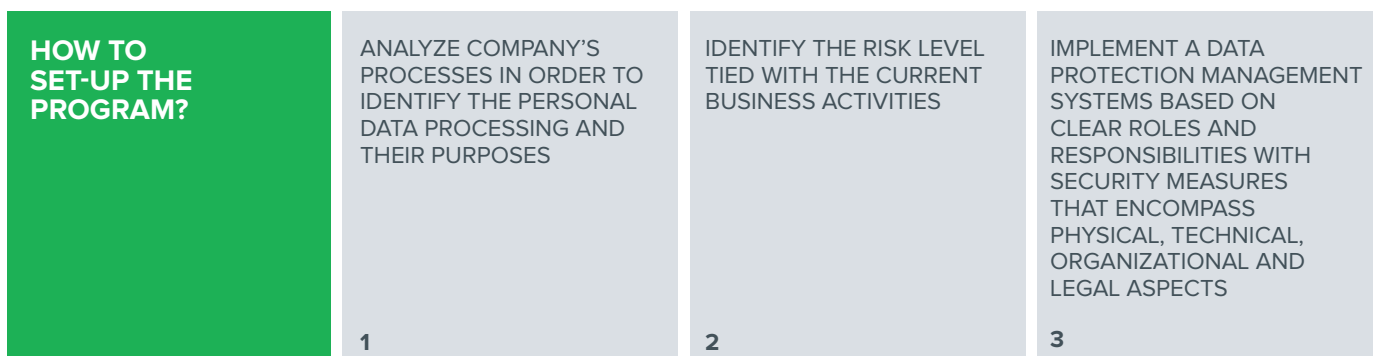
The EU GDPR introduces the concept of “**accountability**” (proof of being compliant) and requires the adoption of a “**risk based approach**”, therefore being compliant with the GDPR requires more than one-off initiatives.

REPLY’s approach is based on the development of a **Privacy and Data Protection Management System** that aims to guarantee confidentiality, integrity and data availability via continuous improvement.

This makes use of international standards and best practices relating to information security and risk management.

## IT WILL BE POSSIBLE TO SHOW THE COMPLIANCE TO THE REGULATION THROUGH CERTIFICATION MECHANISM.

The **Data Protection Management System must be continuously maintained**; each Company is legally obliged to **demonstrate active compliance** with every measure needed to protect data in an appropriate manner.



# HOW WE CAN HELP YOU

Successful GDPR programmes follow a systematic approach. Our team can assist you on all aspects of your GDPR journey, from the assessment of the gaps and the definition of the roadmap to the implementation of all the legal, organizational, procedural and technical solutions necessary to demonstrate compliance, turning privacy compliance into a competitive advantage where possible.

Here is how our team can help to assess, implement and manage your GDPR compliance programme:

## ASSESSMENT

SOLUTION	KEY RESULTS	ELAPSED
<b>ASSESSMENT OF DATA PROTECTION MATURITY AND REMEDIATION PLAN DEFINITION</b>	<ul style="list-style-type: none"><li>• Compliance Requirements mapping</li><li>• Data Protection Framework definition based on GDPR requirements and security best practices</li><li>• Data Protection Maturity evaluation based on the data protection Framework and benchmarking</li><li>• Cybersecurity Maturity Evaluation (optional)</li><li>• Gap identification and compliance risk assessment</li><li>• Recommendation and roadmap for remediation (organization, processes, technologies, legal)</li></ul>	4-12 WEEKS DEPENDING ON THE SIZE AND COMPLEXITY OF ORGANIZATION

## IMPLEMENTATION

SOLUTION	KEY RESULTS	ELAPSED
<b>MANAGEMENT OF A GDPR PROGRAMME</b>	<p>Design and monitoring of data protection program:</p> <ul style="list-style-type: none"><li>• Program definition (tasks, owners, due dates)</li><li>• PMO</li><li>• Work progress report and review</li></ul>	3-24 MONTHS DEPENDING ON MATURITY, SIZE AND COMPLEXITY OF ORGANIZATION
<b>PRIVACY GOVERNANCE</b>	<ul style="list-style-type: none"><li>• Analysis and review of the “responsibility chain” for Controller, Processor and DPO</li><li>• Identification and formalization of DPO required skills, background, role and key responsibilities</li></ul>	4 WEEKS
<b>PERSONAL INFORMATION INVENTORY AND DATA FLOW DISCOVERY</b>	<ul style="list-style-type: none"><li>• Personal data information (structured and unstructured) discovery and data flow documentation using data discovery tools and data governance (MDM, Linage, etc..) best of breed solutions.</li></ul>	4-16 WEEKS DEPENDING ON SIZE AND COMPLEXITY OF ORGANIZATION
<b>PROCESSING ACTIVITIES REGISTER</b>	<ul style="list-style-type: none"><li>• Creation and maintenance of a detailed register of all physical, virtual and logical places where data is held (including e.g. the kind of personal data, the source and who access it)</li><li>• Creation of a CMDB to store processing activities register information (optional)</li></ul>	4-12 WEEKS DEPENDING ON SIZE AND COMPLEXITY OF ORGANIZATION
<b>PRIVACY IMPACT ASSESSMENT/ RISK ASSESSMENT</b>	<ul style="list-style-type: none"><li>• Definition of a risk-driven methodology that includes the management of data across its entire lifecycle - from creation, storage and transfer to removal, including third party suppliers/vendors if present</li><li>• Integration with existing Information Security Risk processes</li><li>• Conduction of a detailed privacy impact assessment on sensitive systems and projects</li><li>• Integration of the KPI / KRI system for privacy</li></ul>	4-12 WEEKS DEPENDING ON SIZE AND COMPLEXITY OF ORGANIZATION

## IMPLEMENTATION

SOLUTION	KEY RESULTS	ELAPSED
<b>SECURITY ASSESSMENT AND DATA PROTECTION SOLUTIONS IDENTIFICATION AND IMPLEMENTATION</b>	<ul style="list-style-type: none"> <li>For each data processing activity, risk-based assessment of the security measures adopted to protect personal data through its lifecycle</li> <li>identification of the technical and procedural solutions to secure personal data through its lifecycle (i.e. IAM/IAG, Data Masking, Encryption, DAM, DLP, etc)</li> <li>Implementation of the identified solutions</li> </ul>	<ul style="list-style-type: none"> <li>4-24 WEEKS DEPENDING ON SIZE AND COMPLEXITY OF ORGANIZATION</li> </ul>
<b>PRIVACY BY DESIGN AND BY DEFAULT PROCESSES DEFINITION</b>	<ul style="list-style-type: none"> <li>Verification of the existence and compliance with GDPR of the main business processes relating to data lifecycle (e.g. demand/change management process)</li> <li>Development of guidelines to address the principles of Privacy by Design and Privacy By Default</li> </ul>	<ul style="list-style-type: none"> <li>4-12 WEEKS DEPENDING ON SIZE AND COMPLEXITY OF ORGANIZATION</li> </ul>
<b>PRIVACY DOCUMENTATION UPDATE</b>	<ul style="list-style-type: none"> <li>Implementation of policies / procedures and definition of the necessary records (e.g. data retention and destruction, response to Data Subjects, consent management, claims, opt-out...)</li> </ul>	<ul style="list-style-type: none"> <li>4-16 WEEKS DEPENDING ON SIZE AND COMPLEXITY OF ORGANIZATION</li> </ul>
<b>INCIDENT MANAGEMENT /DATA BREACH PROCESS DEFINITION/ UPDATE</b>	<ul style="list-style-type: none"> <li>Development of an incident plan (crisis response) to be enacted if data breaches occur. This should include customer response messaging, media response messaging, maximum response times, expected timelines and an outline of all involved parties and their specific crisis-response roles/functions</li> <li>Verification of the procedures to detect, report and investigate a personal data breach</li> <li>Integration with existing incident management processes/ solutions</li> </ul>	<ul style="list-style-type: none"> <li>4-16 WEEKS DEPENDING ON SIZE AND COMPLEXITY OF ORGANIZATION</li> </ul>
<b>THIRD PARTIES MANAGEMENT</b>	<ul style="list-style-type: none"> <li>Analysis of the contracts for data processing (contract renewal, BCR, Privacy Shield, external Data Processors,...)</li> <li>Assessment of the legal criteria for processing non-EU flows</li> <li>Conducting audits on suppliers and any updating of the related contracts</li> </ul>	<ul style="list-style-type: none"> <li>4-24 WEEKS DEPENDING ON SIZE AND COMPLEXITY OF ORGANIZATION</li> </ul>
<b>TRAINING AND AWARENESS</b>	<ul style="list-style-type: none"> <li>Training and awareness to employees across the organization, outlining breach scenarios and causes, explaining record keeping/monitoring best practices and providing an overview of proper data protection practices.</li> </ul>	<ul style="list-style-type: none"> <li>4-16 WEEKS DEPENDING ON SIZE AND COMPLEXITY OF ORGANIZATION</li> </ul>

## MANAGEMENT

SOLUTION	KEY RESULTS	ELAPSED
<b>SPECIALISTIC SUPPORT FOR ONGOING PROGRAM MANAGEMENT</b>	<p>Ongoing compliance and monitoring support:</p> <ul style="list-style-type: none"> <li>Conduct DPIAs for each new project/services</li> <li>Manage a Data Processing Activities Register (ongoing update)</li> <li>Periodic assessment on the processed data and related security measures across the organization or within particular business areas</li> <li>Periodic audits on suppliers and any updating of the related contracts</li> <li>Assessment of employees awareness (e.g. assessment tests, incident simulation exercises, ...)</li> <li>TBD ACCORDING TO PROGRAM ACTIVITIES</li> </ul>	<ul style="list-style-type: none"> <li>TBD ACCORDING TO PROGRAM ACTIVITIES</li> </ul>





## TIPS

Have you already started working on GDPR?

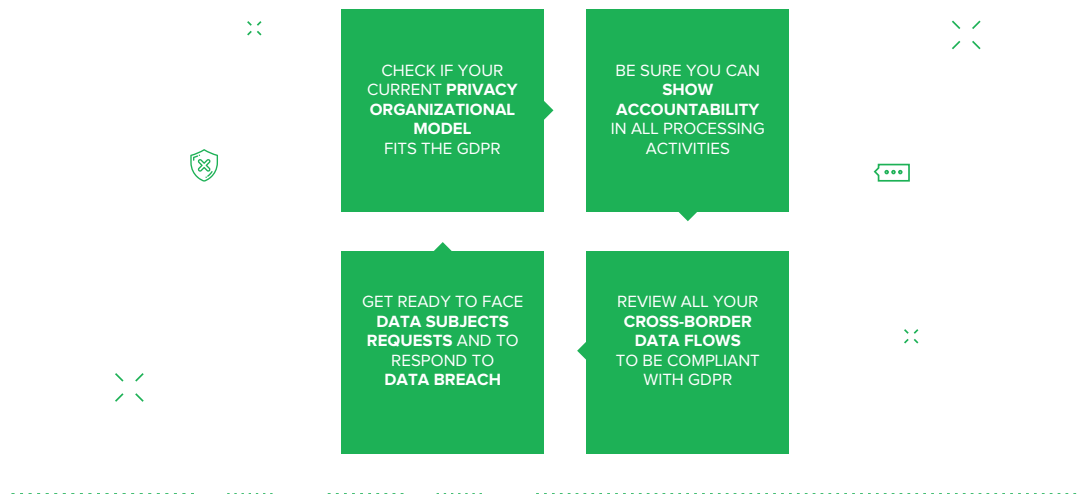
The following provides some tips to check if you are on the right path to compliance.

### THE GDPR JOURNEY

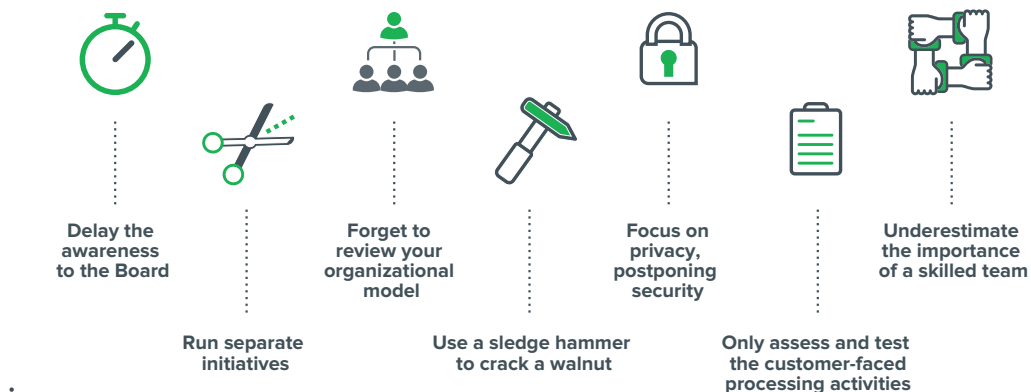




## DOs



## DON'Ts



## ONE REGULATION, MANY POINTS OF VIEW

<b>DATA PROTECTION AUTHORITY</b>	Is the Governance Framework complete? Are practices aligned to it? Are roles assigned? <b>Can you show evidences of effectiveness?</b> Is a remediation plan defined for breaches?	<b>EXTERNAL</b>
<b>CUSTOMERS</b>	Can you delete my data? Why are you contacting me without consent? Why did you disclose my data I erased some time ago? <b>Who are the third parties processing my data, and where?</b>	
<b>GDPR PROGRAM MANAGER</b>	Are task ownerships assigned? Are task dependencies clear? Are goals achievable? <b>Are criticalities addressed?</b> Is the working team skilled? Is the program adequately endorsed?	<b>INTERNAL</b>
<b>CTO, CDO, CSO, CISO</b>	Do applications store audit trails to enforce breach prevention and management? Are user access rights and profiles validated? <b>Is data protected adequately from collection to erasure?</b>	
<b>LEGAL, PRIVACY OFFICE, COMPLIANCE</b>	Are privacy risks assessed? Are employees aware of their duties and responsibilities? <b>Are company practices on data compliant with policies and notices?</b> How long is data retained?	





# WHY REPLY?



## WITH EXTENSIVE EXPERIENCE IN DATA PROTECTION, PRIVACY, COMPLIANCE AND GOVERNANCE REPLY CAN:

OFFER OUR MIX OF GOVERNANCE, COMPLIANCE, TECHNOLOGY AND SYSTEM INTEGRATION SKILLS - TO HELP YOU ON YOUR COMPLIANCE JOURNEY FROM ASSESSMENT TO IMPLEMENTATION;

PROVIDE OUR PROVEN APPROACH FROM A WIDE RANGE OF INTERNATIONAL SUCCESS STORIES;

TRANSFER ALL THE KNOW-HOW REQUIRED TO CONTINUOUSLY OPERATE, MAINTAIN AND IMPROVE GDPR PROGRAM;

GUIDE THE CUSTOMER DURING THE CHOICE OF SUITABLE TECHNICAL SECURITY MEASURES AND SUPPORT THEIR IMPLEMENTATION;

PROVIDE A TEAM OF HIGHLY COMMITTED CONSULTANTS.







**Sonia Crucitti**

Partner | ITALY

phone: +39 02 535761

s.crucitti@reply.it



**Marco Graia**

Manager | GERMANY

phone: +49 211 339905-0

m.graia@reply.it



**Alessandra Mariz**

Manager | UK

phone: +44 (0)20 7730 6000

a.mariz@reply.com



**Astrid Froidure**

Associate Partner | BENELUX

phone: +32 476 88 70 98

a.froidure@reply.com



**Reply** specialises in the design and implementation of solutions based on digital media and new communication channels. Through its network of highly specialised companies, Reply partners with major European corporations in the telecoms and media, industry and services, banking and insurance, and public administration sectors, to devise and develop business models built on the new paradigms of big data, cloud computing, digital media and the Internet of Things. Reply's services include: Consulting, Systems Integration and Digital Services.

**[www.reply.com](http://www.reply.com)**