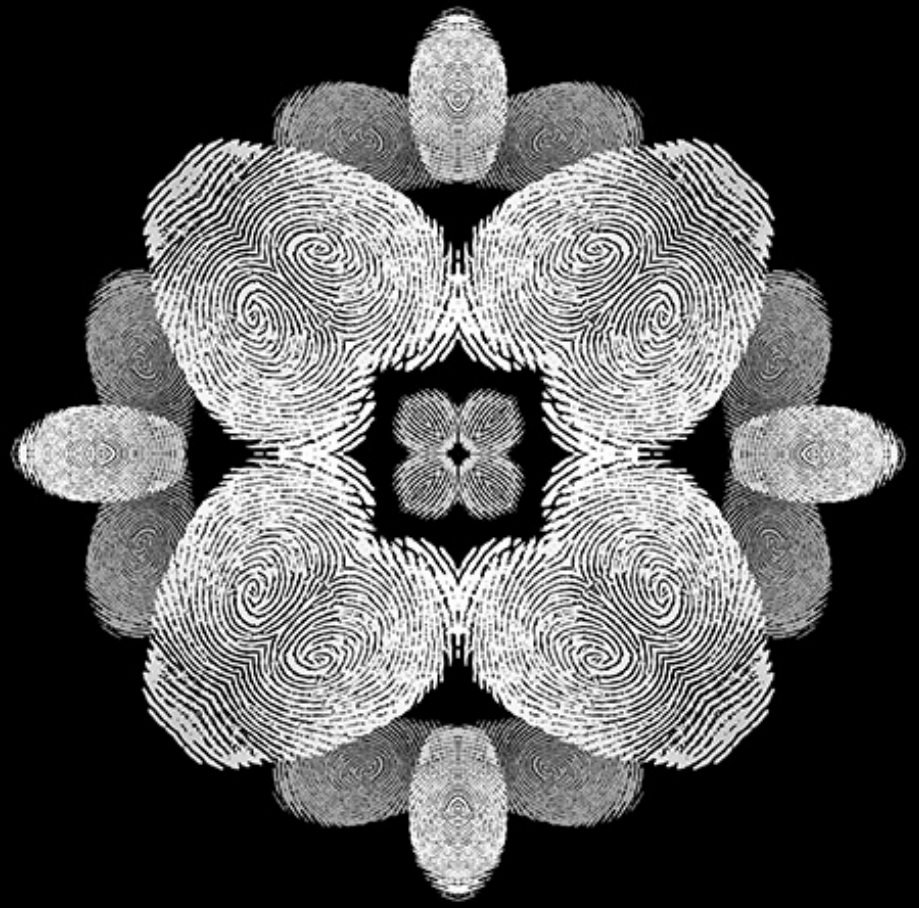
Deloitte.



General Data Protection Regulation (GDPR)

Deloitte Malta Privacy Services

Deloitte Risk Advisory 2018

General Data Protection Regulation (GDPR)

Overview

- The General Data Protection Regulation (GDPR) will come into effect on 25 May 2018, changing the European privacy landscape. For organisations, this means a number of changes. In this brochure we outline some major points from our experience that can help organisations to make the most of these changes.
- Organisations have to identify how this new legislation may impact them. This will of course vary per organisation, but in general terms, privacy compliance goes well beyond addressing legal matters. Complying with this new regulation is likely to involve putting new governance arrangements in place, modifying existing processes and the implementation of new technological measures.
- GDPR affects absolutely every company, which processes personal data in its everyday business – be it clients' data or even the data of its own employees. It is also crucial to note that GDPR does not merely concern companies established in the EU, but also those that process data of EU data subjects – for example, companies offering their products or services to the EU market.
- Deloitte has comprehensive international experience in the field of data protection and is able to help bring the internal processes of your organisation in compliance with GDPR requirements.
- In the meantime, should you have any specific question on the GDPR or privacy and data protection within your organisation, please contact the Deloitte Malta Privacy Team illustrated on page 19.

The big picture

Key changes of the GDPR

Fines of up to 4% of annual global turnover

€'000 → €'000,000

Previously fines were limited in size and impact. GDPR fines will apply to both controllers and processors.

Increased territorial scope

GDPR will apply to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location.

Explicit and retractable consent

Must be provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Right to access and portability

Data subjects can request confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.

Breach notification within 72 hours

Now mandatory that breaches, which are likely to "result in a risk for the rights and freedoms of individuals", are reported within 72 hours of first having become aware of the breach.

Privacy By Design

Now a legal requirement for the inclusion of data protection from the onset of the designing of systems, rather than a retrospective addition.

Right to be forgotten

Entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

Mandatory Data Protection Officers

Appointed in certain cases (public authorities, when monitoring of data subjects on a large scale and when processing special categories of data). To facilitate the need for a company to demonstrate their compliance to the GDPR and compensate for GDPR no longer requiring the bureaucratic submission of notifications/ registrations of data processing activities or transfers based on Model Contract Clauses.

Deloitte perspective on GDPR

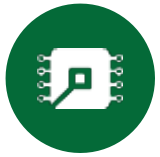
Organisational perspectives

GDPR impacts many areas of an organisation: legal and compliance, technology, and data

Legal and compliance: The GPDR introduces new requirements and challenges for legal and compliance functions. Many organisations will require a Data Protection Officer (DPO) who will have a key role in ensuring compliance. It is estimated that 28,000 new DPOs will be required in Europe alone. If the GDPR is not complied with, organisations will face the heaviest fines yet – up to 4% of global turnover. A renewed emphasis on organisational accountability will require proactive, robust privacy governance, requiring organisations to review how they write privacy policies, to make these easier to understand.

Who should care:

- General Counsel
- Privacy Office
- Chief Risk Officer
- Chief Compliance officer



Technology: New GDPR requirements will mean changes to the ways in which technologies are designed and managed. Documented privacy risk assessments will be required to deploy major new systems and technologies. Security breaches will have to be notified to regulators within 72 hours, meaning implementation of new or enhanced incident response procedures. The concept of 'Privacy By Design has now become enshrined in law, with the Privacy Impact Assessment expected to become commonplace across organisations over the next few years. And organisations will be expected to look more into data masking, pseudo-anonymisation and encryption.

- Chief Information Officer
- Chief Information Security Officer

Data: Individuals and teams tasked with information management will be challenged to provide clearer oversight on data storage, journeys, and lineage. Having a better grasp of what data is collected and where it is stored will make it easier to comply with new data subject rights – rights to have data deleted and to have it ported to other organisations.

- Chief Data Officer
- Chief Operating Officer

Perspective: Legal and compliance

General Counsels, Chief Compliance Officers, Chief Privacy Officers and Data Protection Officers: Your privacy strategies, resourcing, and organisational controls will need to be revised. Boardrooms will need to be engaged more than ever before.

A revolution in enforcement

Fines of up to 4% of annual global turnover

Serious non-compliance could result in fines of up to

4% of annual global turnover, or €20 million – whichever is higher. Enforcement action will extend to countries outside of the EU, where analysis on EU citizens is performed. But how will this play out in practice? Will US organisations, for example, take heed of EU data protection authorities?

Data protection officers

Market hots up for independent specialists

Organisations processing personal data on a large scale will now be required to appoint an independent, adequately qualified Data Protection Officer. This will present a challenge for many medium to large organisations, as individuals with sought-after skills and experience are currently in short supply. Organisations will also be challenged to demonstrate an independent reporting line, which could cause issues with incumbent positions.

Accountability

Burden of proof now on the organisation, not the individual

The current requirement to provide annual notifications of processing activities to local regulators will be replaced by significant new requirements around maintenance of audit trails and data journeys. The focus is on organisations having a more proactive, comprehensive view of their data and being able to demonstrate they are compliant with the GDPR requirements.

Privacy notices and consent

Clarity and education is key

Organisations will now consider carefully how they construct their public-facing privacy policies to provide more detailed information. However, it will no longer be good enough to hide behind pages of legalese. In addition, there is a significant shift in the role of consent, with organisations required to obtain ‘freely given, specific, informed and unambiguous’ consent, while being able to demonstrate these criteria have been met.

Perspective: Technology

Chief Information Officers, Chief Technology Officers and Chief Information Security Officers: Your approach towards the use of technology to enable information security and other compliance initiatives will need to be reconsidered, with costs potentially rising.

Breach reporting

Breach reporting within 72 hours of detection

Significant data breaches will now have to be reported to regulators and in some circumstances also to the individuals impacted. This means organisations will have to urgently revise their incident management procedures and consider processes for regularly testing, assessing and evaluating their end to end incident management processes.

Encryption

Encryption as means of providing immunity?

The GDPR formally recognises the privacy benefits of encryption, including an exemption from notifying individuals of data breaches when data is encrypted. However, this does not mean that organisations can afford to be complacent, and the exemption may not apply when weak encryption has been used. Given the potential fines, organisations will have to further increase their focus on a robust information and cyber security regime.

Online profiling

Profiling becomes a loaded topic

Individuals will have new rights to opt out of and object to online profiling and tracking, significantly impacting direct-to-consumer businesses who rely on such techniques to better understand their customers. This applies not just to websites, but also to other digital assets, such as mobile apps, wearable devices, and emerging technologies.

Privacy by design

Recognised best practice becomes law

The concept of Privacy By Design (PbD) is nothing new, but now it is enshrined in the GDPR. Organisations need to build a mind set that has privacy at the forefront of the design, build and deployment of new technologies. One manifestation of PbD is Data Protection Impact Assessments (DPIA), which are now required to be undertaken for new uses of personal data where the risk to individuals is high.

Perspective: Data

Chief Data Officers, Data Stewards, Chief Marketing Officers, and Digital Leads: Your information management activities have always supported privacy initiatives, but under the GDPR new activities are required which specifically link to compliance demands.

Data inventories

Identifying and tracking data

Organisations will have to take steps to demonstrate they know what data they hold, where it is stored, and who it is shared with, by creating and maintaining an inventory of data processing activities. Data leads will have to work closely with privacy colleagues to ensure all necessary bases are covered. A thorough system for maintaining inventories needs to be implemented.

Right to be forgotten

A stronger right for consumers to request deletion of their data

A new 'right to be forgotten' is further evidence of the consumer being in the driving set when it comes to use of their data. Depending on regulatory interpretation, organisations may need to perform wholesale reviews of processes, system architecture, and third party data access controls. In addition, archive media may also need to be reviewed and data deleted.

Right to data portability

A new right to request standardised copies of data

A new right to 'data portability' means that individuals are entitled to request copies of their data in a readable and standardised format. The interpretation of this requirement is debatable, but taken broadly the challenges could be numerous – amongst them achieving clarity on which data needs to be provided, extracting data efficiently, and providing data in an industry-standardised form.

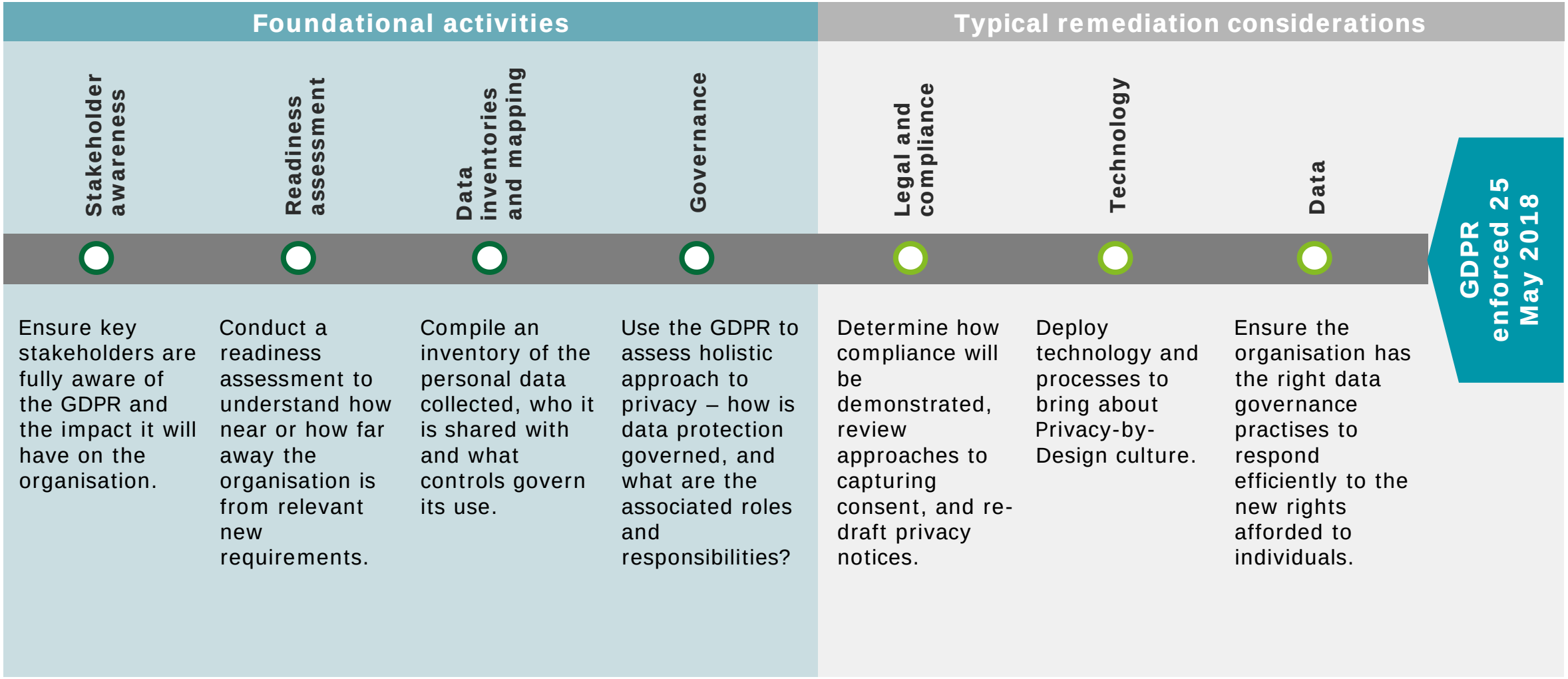
New definitions of data

New concept of pseudo-anonymous data

The GDPR recognises the concept of pseudo-anonymous data and at the same time expands the definition of personal data, placing an greater emphasis on data classification and governance. But it remains unclear if and when certain data, for example IP addresses, will be classed as personal data and subject to requirements.

Key activities and considerations

To reach GDPR compliance, both foundational and remedial activities are required.



Our services

Our key privacy and data protection areas

We have a dedicated team of privacy professionals, with thorough expertise in leading privacy programmes across large scale and complex organisations

Compliance and readiness	Privacy programmes	Technology and data	Risk management	Training and cultural change	Cyber security
• GDPR readiness assessment • GDPR compliance • roadmap • Global privacy compliance assessment • GDPR technology impact assessment • Global compliance assessments	• Privacy programme development • Privacy strategy and roadmap development • Target operating model design and implementation • Change programme design and delivery	• Data discovery, mapping, and inventories • Privacy-by-design advice and application • Online and e-privacy • Digital asset risk assessment and management (e.g. websites and mobile apps)	• Privacy impact assessment and health check • Policy analysis and • design • Governance and compliance review • Third party management	• Privacy risk and compliance training • Training and awareness design and implementation • Classroom based training • Cultural change programme development	• Personal data breach investigation and management • Regulatory liaison advice • Incident response and forensic investigation support • Supplier and third party management

We have experience with performing assessments of organisation's readiness based on GDPR requirements, among others.	We designed and developed a group-wide privacy programmes for a banking client.
Our deliverables help organisations to gain a better insight in their processes regarding privacy, such as: formal reports, governance models, policies and processes, and roadmaps.	We supported the implementation of a privacy roadmap for a banking client.

Actions to take to prepare for the GDPR

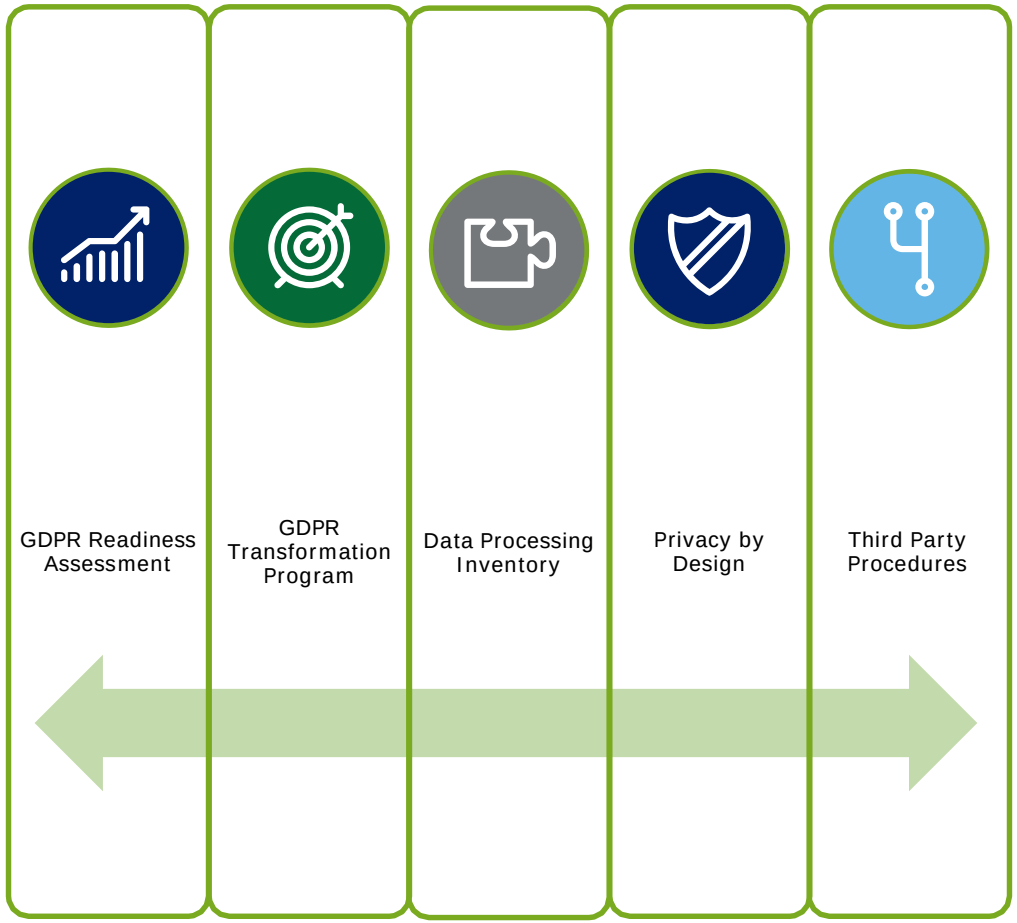
GDPR Readiness Assessment

GDPR Transformation Program

Data Processing Inventory

Privacy by Design

Third Party Procedures



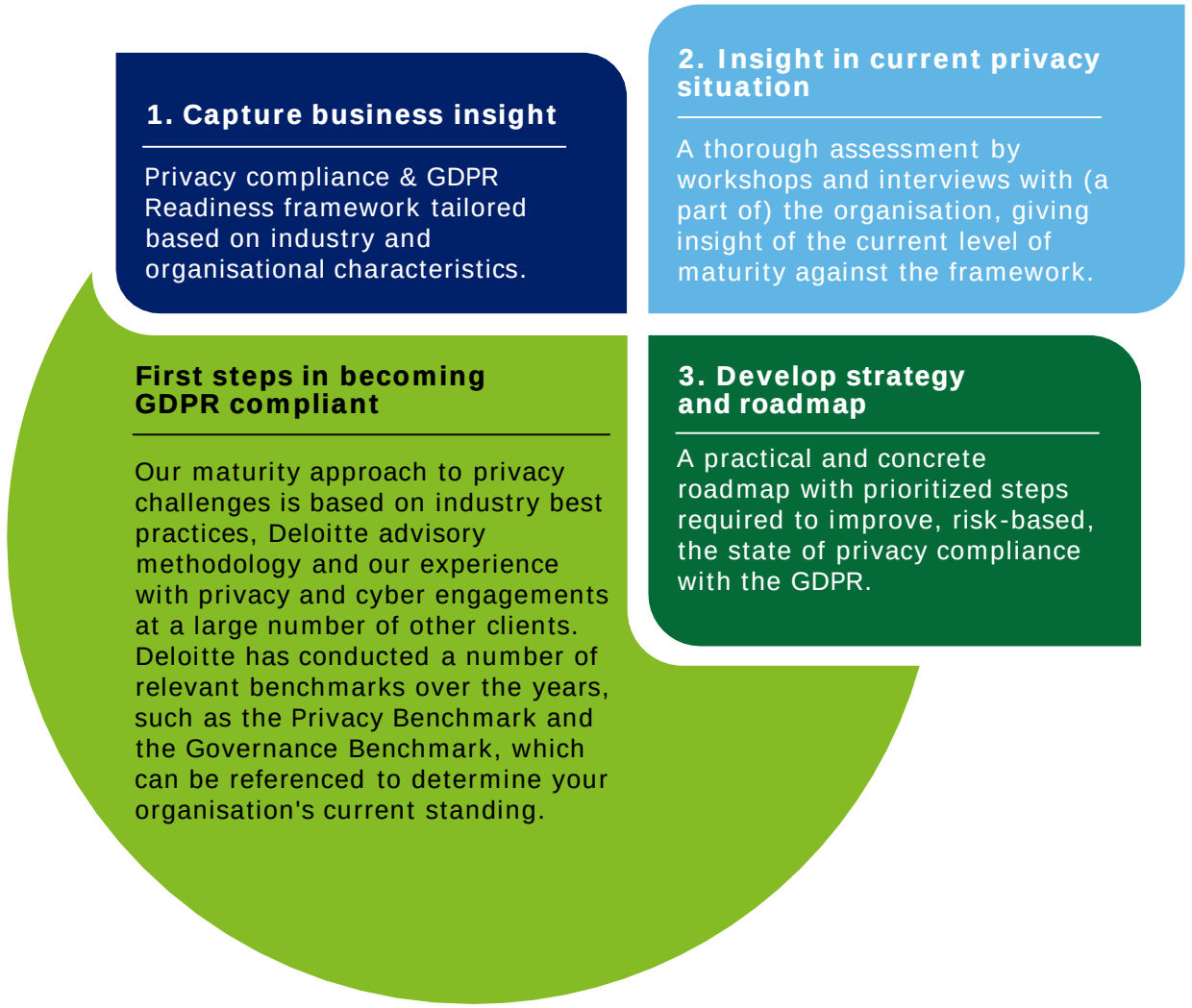
GDPR Readiness Assessment

The road to GDPR compliance with the GDPR Maturity Assessment & Roadmap

What is the GDPR Readiness Assessment?

To give a clear picture on where your organisation currently stands with respect to the GDPR, the GDPR Readiness Assessment is the tool of choice. The GDPR Readiness Assessment is:

- A powerful tool, based on an existing Deloitte platform to create a baseline for privacy.
- Part of the cyber tooling suite, potential to incorporate into your broader cyber strategy and roadmap.
- Used by Deloitte globally for privacy and cyber assessments and strategy definition.
- A good starting point for becoming compliant with the GDPR and getting a tailored privacy program.
- Based on our Privacy, Security and Governance framework, covering all elements of the described privacy program.
- Instrumental in finding the areas with the biggest risk.
- Used to focus on those areas which most urgently need action to become GDPR compliant.
- A method to measure how mature the organisation currently is, using the Deloitte privacy and data protection maturity model.

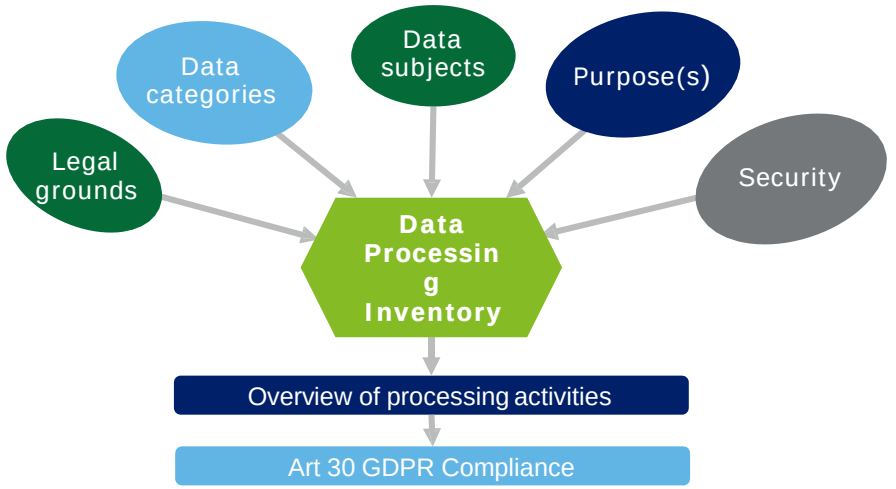


GDPR Processing Inventory

Creating a data inventory provides an overview of all data and insights in the risks attached to processing activities

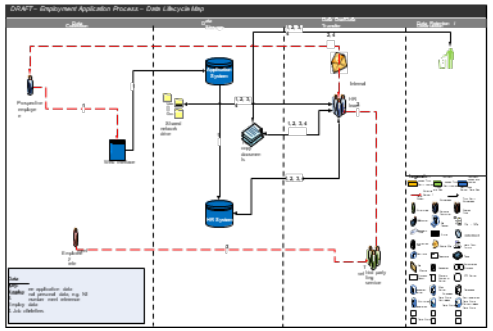
A Data Processing Inventory is your basis to get in control of your data processing

- A data inventory is an overview which includes all the required information concerning personal data processing, such as legal grounds, purpose(s), categories of data, retention period and conducted risk analysis.
- Having an inventory is an actual requirement under the GDPR (following from **article 30**), but it can also serve you well in building your understanding of the personal data you processes.
- The inventory is used as a register of all the data processes within the organisation. Having an inventory is essential for your oversight of processing activities and is a mandatory element of GDPR compliance.
- The inventory allows your organisation to demonstrate awareness of its obligations as a data controller, including keeping of records of processing activities.
- Finally, knowing which personal data the organisation processes mitigates the risk of unidentified data breaches.



In data mapping, there are two stages: the data capture template and the data map flowchart.

Data capture template



Data map flowchart

Privacy by Design

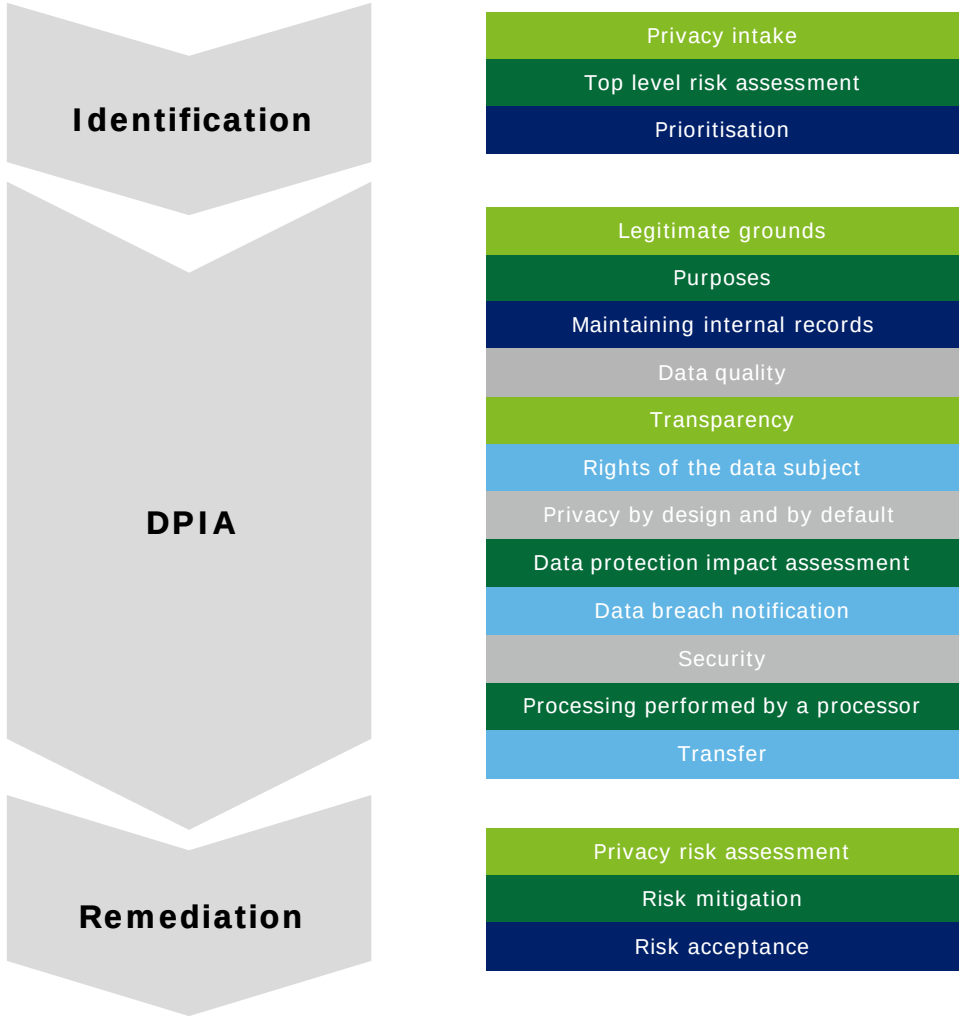
Embedding privacy into your project methodology by assessing privacy risks in an early stage

A tailored approach

Privacy can be considered as an operational risk that requires practical solutions in order to make sure that risk is actually handled. The challenge is to provide uniform and flexible methodologies and process to safeguard privacy every time a data driven project starts.

Key elements to consider

- Ensuring new projects and initiatives abide by the privacy rules within your organisation is done through a robust Privacy by Design (PbD) approach.
- Data Protection Impact Assessments (DPIAs) are based on the GDPR and are a proven and effective tool to assess privacy risks.
- A PbD approach consists of a number of elements: a PbD process, DPIA method, and a remediation framework:
  - The DPIA process describes the phases of identification, DPIA and remediation covering roles, responsibilities, sign offs, escalation, support for a DPIA and should be efficient and effective.
  - A DPIA method is the combination of checks, questions and requirements to assess the impact and risks that any system or project should follow.
  - Remediation should always be the end phase of privacy by design and makes sure impact can be reduced and risks mitigated or accepted.



Third Party Procedures

External parties bring specific challenges for data controllers

Data Breach Handling Procedure

When a data breach occurs there are many internal and external challenges. Handling and communication procedures with processors, authorities and data subjects are essential for effective data breach handling.

Data Processing Agreements (DPAs)

Are your DPAs GDPR proof? With the new data breach rules in place there is a requirement for contractual arrangements between Controller and Processors.

Vendor Assessment

Every time your organisation uses a third party for any kind of service that might involve data processing there should be a concrete process with clear requirements to assess these parties and their specific service.

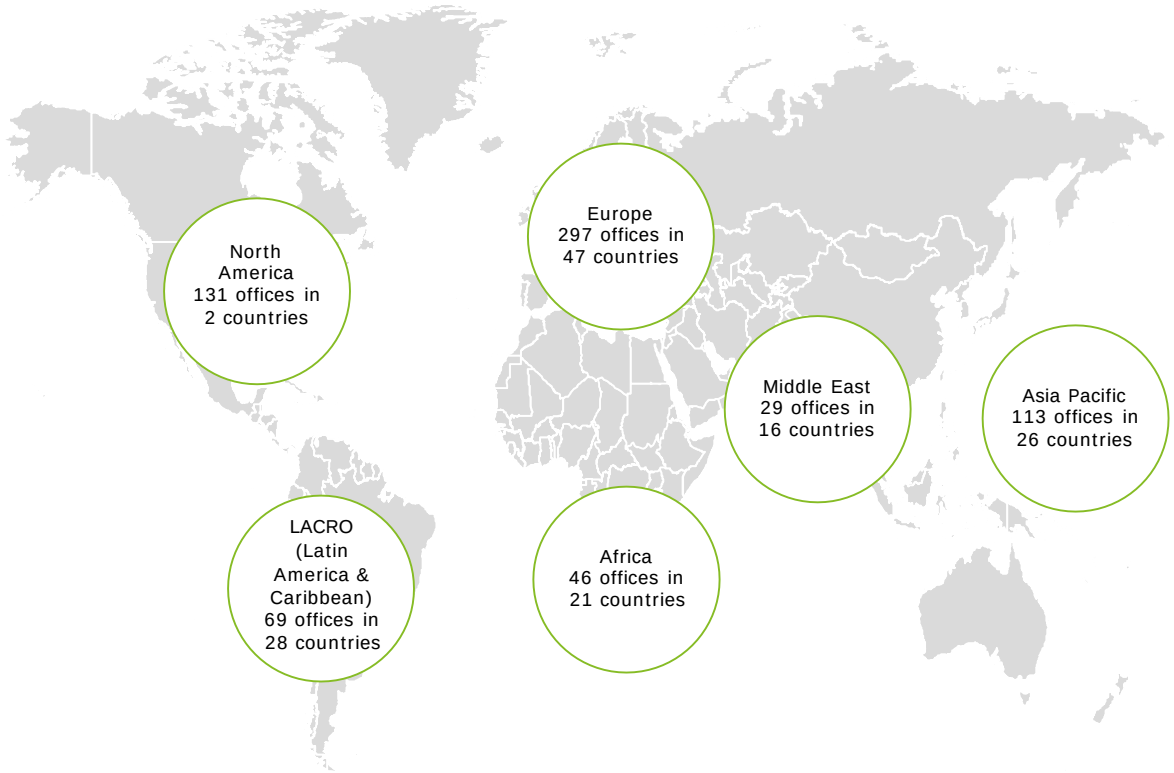
To make sure this is done effectively there needs to be collaboration between legal, risk, IT and procurement with strong steering
from the DPO.

Data Subject Rights procedure

The most important external stakeholder are your data subjects. The GDPR brings increased rights to data subjects (customers, patients, citizens) and this brings procedural challenges to a controller. Whether a data subject requests access, erasure or portability of their data, a good process on how to communicate and serve these data subjects is essential.

Why Deloitte?

Deloitte is the largest global professional services firm and recognised leader in the privacy and security domain



Ratio

Over 200,000 professionals in almost 140 countries share extensive knowledge and experience, which facilitates a unified approach in delivering the highest quality of services.

- More than 12,000 IT risk consultants and 3,000 security professionals worldwide;
- Analysts praise our ability to execute and tackle difficult challenges:
  - ✓ *"Deloitte's ability to execute rated the highest of all the participants."*
  - ✓ *"…Deloitte shines when tackling large-scale challenges at mature, complex organisations. Customers facing such issues and looking for a vendor that will marry deep technical capabilities with strong business processes should look to Deloitte."*

Accreditations

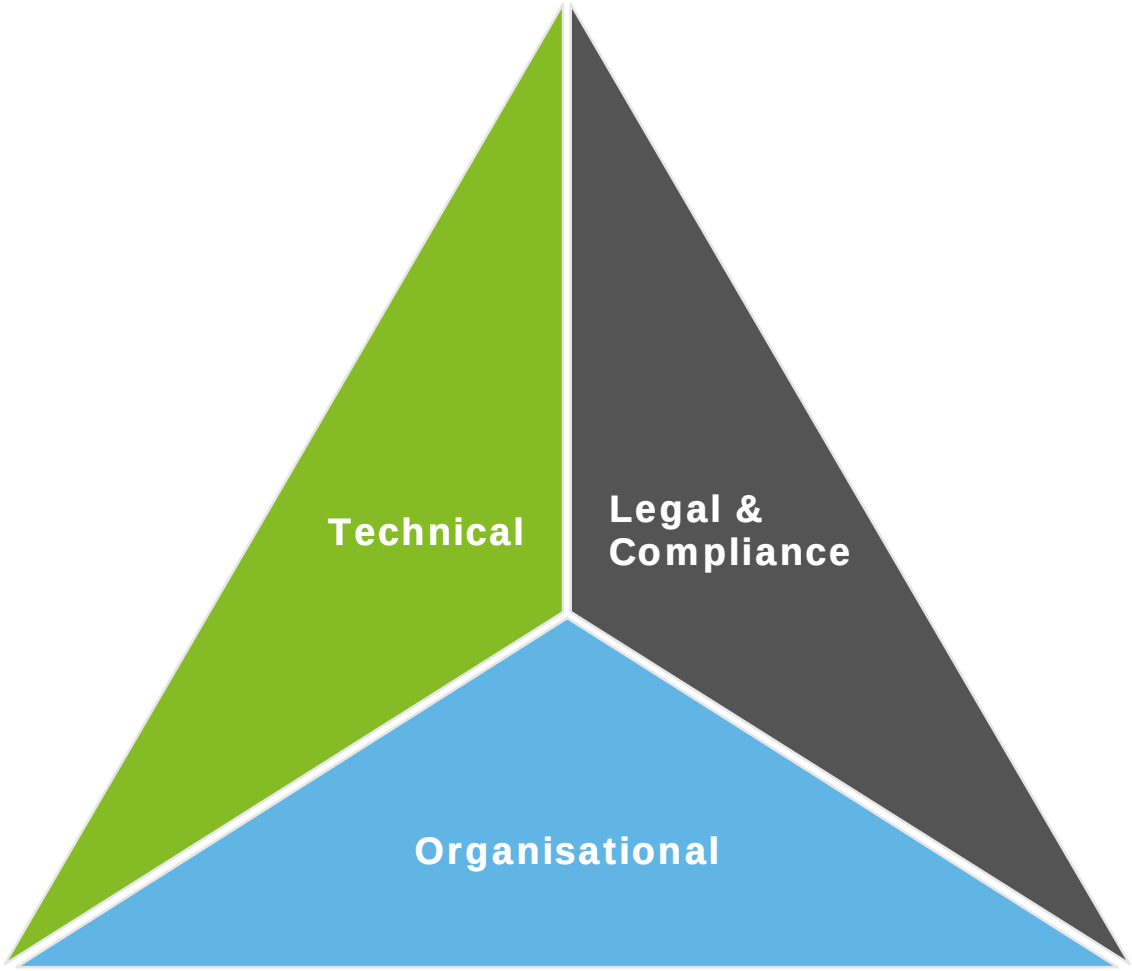
ISC^2	Over 1,100 CISSPs
ISACA	Over 2,000 certified as CISA, CISM, GEIT
BSI	Over 150 trained lead systems auditors
IAPP	Privacy certified practitioners
Speciality	Wide range of domain specific certifications
PMI	PMI certified practitioners

Deloitte vision on privacy

Why our team is unique

Key focus areas

- Deloitte has an international privacy organisation and is well positioned to cross-border engagements.
- Deloitte Privacy Services is the market leader in Europe for privacy advisory services.
- In order to address privacy challenges correctly, these three focus areas (technical, legal & compliance, and organisational) in your organisation need to be involved. The team consists of experts on each of those fields.
- We have a wide range of services geared towards protecting privacy and our client's interests.
- We have a wealth of experience servicing clients in multiple industries.
- We are a major supplier of privacy training and education (Privacy Officer training, CIPP).
- We organise leading events on privacy such as Data with a View and GDPR Expert talks.
- Our buyers and sponsors range from CPO, CIO and CLO to strategy executives and the business.



Contacts

For more information, please contact us.

Stephen Paris
Director
Deloitte Risk Advisory
sparis@deloitte.com.mt

Ivan Spiteri
Senior Manager
Deloitte Cyber Risk Services
ispiteri@deloitte.com.mt

Learn more on GDPR: www.deloitte.com/mt/gdpr

Deloitte.