

Understanding the General Data Protection Regulation (GDPR)

A short walk through of the key aspects

Deloitte Malta Risk Advisory, 2018

Regulatory Risk



Introduction

Organisations must meet the demands of the complex regulatory landscape, but be flexible enough that the regulatory programme keeps pace with a rapidly changing environment—all with an industry-focus.

Is your approach to regulatory risk designed to preserve value and power performance?

Our services

Deloitte helps organisations anticipate and adapt to changes in the regulatory environment, and build better programmes and controls to address the wide variety of regulations and regulatory risks. We work with clients and regulators on effective remediation in response to accountability and compliance events.

Regulatory strategy

We develop regulatory strategies, structures, and processes that enable a proactive, forward looking assessment of regulatory trends and their impact on business models.

Regulatory response

We help clients respond to specific breakdowns in their regulatory accountability and compliance programmes which are often driven by actual, or the prospect of, regulatory censure.

Regulatory compliance

We assist clients in designing, assessing, and transforming their enterprise compliance programmes to preserve organisational value and create competitive advantage.

Overview of the GDPR

Half of all firms still not compliant with 1998 data laws



How does the EU GDPR impact organisations in Malta?

The changes will have a profound impact on the operational and control environment of organisations.

The GDPR is expected not only to impact organisations within the EU, but also those organisations globally with:



Operations within the EU



Third parties operating in the EU



EU citizens as customers

Most organisations will be able to attest to the effort and project(s) which were undertaken to prepare for the implementation of the Data Protection Act 2001 [CAP 440].

Organisations should not underestimate the time it will take to comply with these changes.



Overview of the main changes

55k

Thousands of words making up the text of the GDPR

7

Core individual rights afforded under the GDPR

72

Hours given to report a data breach

250m

Cost of 4% fine for a typical FTSE 100 company

28k

Estimated number of new Data Protection Officers required in Europe (IAPP study 2016)

190+

Countries potentially in scope of the regulation

80+

New requirements in the GDPR

Data Protection Regulation: No Longer a Paper Tiger

Key risks



Damage of reputation



4% Loss in income



Regulatory enforcement

Breach of regulation



Businesses must notify the authorities of a data breach within 72 hours to avoid a fine up to €10 million.



If a business stores its data on non-EEA servers, it also needs to comply with GDPR to avoid a fine up to €20 million.

GDPR requirements fall into five areas

1. Data governance	The tone on the top, policies, roles, responsibilities, and organisational structures support the protection of individuals' privacy.	GDPR requirements that are generally implemented centrally and can be assessed once for the entire organisation.
2. Data subject rights	Controllers gives individuals ("data subjects") control over what data is processed about them and for what purpose.	
3. Security of personal data	Personal data is processed securely; authorities and where applicable data subjects are notified of high-risk breaches.	
4. Data transfers	Legal and procedural controls are in place to ensure the adequate protection of personal data by third parties.	
5. Data protection principles	Business and HR processes are such that the processing of personal data is lawful, purpose-limited, and transparent to the data subject .	GDPR requirements that are generally implemented by each HR and Business Process separately and consequently, must be assessed on a process-by-process basis.

The GDPR check points

- ☐ Becoming aware
- ☐ Becoming accountable
- ☐ Communicating with staff
- ☐ Personal privacy rights
- ☐ Access request change
- ☐ Legal basis
- ☐ Consent
- ☐ Children and minors
- ☐ Breaches
- ☐ Data protection impact assessments
- ☐ Data protection officers
- ☐ International organisations

Who does the GDPR apply to?

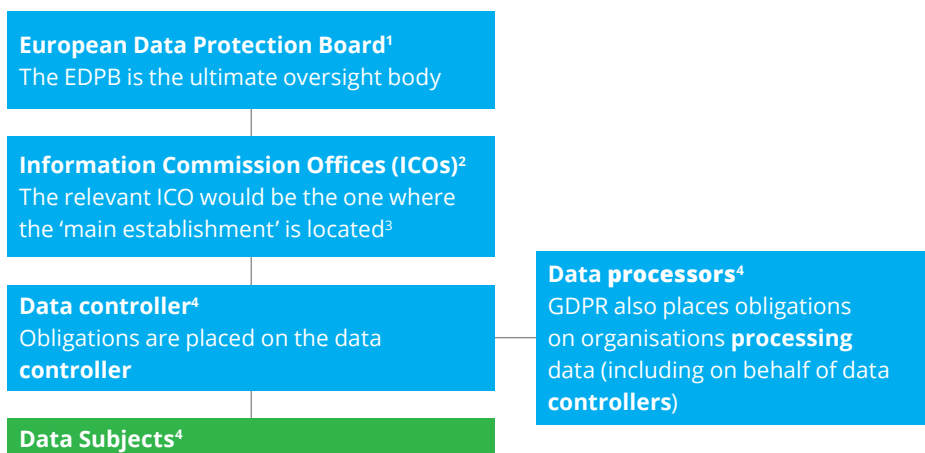
Territorial scope

The GDPR applies if an entity is established in the EU, and is engaged in the **processing** of personal data in the context of that establishment's activity, even if the **processing** itself takes place outside the EU. The GDPR also applies to entities without an establishment in the EU if they process personal data of EU **data subjects**, and the data relates to goods or services offered to EU **data subjects** or the monitoring of behaviour in the EU.

Material scope

The GDPR applies to the electronic or automated **processing** of personal data and to manual paper based **processing** if the personal data forms part of, or is intended to form part of, a filing system.

General Data Protection Regulation Basics



¹ The EDPB will replace the Article 29 working group. It is yet to be set up.

² In Malta this is the office of Information and Data Protection Commissioner (IDPC).

³ The country where the **controller** or **processor** are located. Where, however, the **controller** or **processor** have establishments in more than one Member State (MS).

a. **Controller**, the place of its central administration in the EU, unless the decision on the purposes and means of the **processing** of personal data are taken in another establishment of the **controller** in the EU and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is considered to be the main establishment.

b. As regards to a **processor**, the place of its central administration in the EU, or, if the **processor** has no central administration in the EU, the establishment of the **processor** in the EU where the main **processing** activities in the context of the activities of an establishment of the **processor** take place to the extent that the **processor** is subject to specific obligations under the CDPR.

⁴ Definitions can be found in Article 4 of the Regulation.

Key definitions

Personal data Article 4(1) of GDPR	Any information relating to an identified or unidentified natural person (" data subject "); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Processing Article 4(2) of GDPR and Article 4(7) of GDPR	Any operation which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure or by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction or even mere storage.
Special categories of data⁴	Special categories of data are 'sensitive' data.
(Data) controller Article 4(8) of GDPR	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by EU or MS law, the controller or the specific criteria for its nomination may be provided for by a EU or MS law.
(Data) processor Article 4(8) of GDPR	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller .

When is the GDPR not applicable to the processing of personal data?

- By a natural person in the course of a purely personal or household activity (the "household exemption").
- Concerning the personal data of deceased persons.
- By competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of threats to public security.
- By EU institutions where a unique Regulation for **processing** personal data by EU institutions will continue to apply instead of the GDPR.
- In the course of an activity which falls outside the scope of EU law (e.g. activities concerning national security).
- Relating to the EU's common foreign and security policy.

Article 5 of the GDPR: "Principles relating to processing of personal data"

Personal data shall be:

- Processed **lawfully, fairly** and in a **transparent** manner in relation to the **data subject** ('**lawfulness, fairness and transparency**');
 - Collected for **specified, explicit** and **legitimate** purposes and not further processed in a manner that is incompatible with those purposes; further **processing** for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), is not considered to be incompatible with the initial purposes ('**purpose limitation**');
 - Adequate, relevant** and **limited** to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');
 - Accurate** and, where necessary, **kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**');
 - Kept in a form which permits identification of **data subjects** for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the **data subject** ('**storage limitation**');
 - Processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful **processing** and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**').

High level check list

	Actions	GDPR Articles
Governance	<ul style="list-style-type: none"> Document your Privacy Governance Model - e.g. with clear roles and responsibilities and reporting lines to embed privacy, accountability and compliance into the organisation. Consider whether a statutory (Data Protection Officer) DPO is required. If no EU presence, appoint a local representative. Develop and roll out training across all personnel. Review insurance coverage and consider whether it needs to be updated in light of the higher fines and penalties under the GDPR. 	5, 27, 37-39
Accountability	<ul style="list-style-type: none"> Implement a global overarching data protection policy, which brings together all underlying related policies including processes for privacy by design, and the creation and maintenance of a record of processing activities. Integrate privacy compliance into the audit framework. 	5, 24, 25, 30
Fair processing and consent	<ul style="list-style-type: none"> Review your existing grounds for lawful processing and confirm that these will still be sufficient under the GDPR - e.g. can you still rely on consent given by a client under the Data Protection Act [CAP 440] (DPA). Consider whether your organisation is processing any sensitive personal data. Ensure systems can accommodate withdrawal of consent. 	5, 6, 7, 9, 10, 81-91
Children	<ul style="list-style-type: none"> Identify whether you process personal data of children. If data relating to a child is processed, ensure that notices directed at that child are "child-friendly" and if consent is relied upon, you have implemented a mechanism to seek parental consent. Consider alternative protections - e.g. age-gating. 	12-14
Privacy by design and default	<ul style="list-style-type: none"> Ensure processes are in place to embed privacy by design into projects - e.g. technical and organisational measures are in place to ensure data minimisation, purpose limitation and security. Put in place a privacy impact assessment protocol. 	25, 35, 36
Compliant contracting	<ul style="list-style-type: none"> Develop compliant contract wording for customer agreement and third-party vendor agreements. Identify all contracts that require relevant contract wording, prioritise and develop process for amending. Ensure procurement process has controls to ensure privacy by design - e.g. security diligence, data minimisation, visibility of onwards data flows. 	
Data breach procedures	<ul style="list-style-type: none"> Review and update (or develop where not in existence) a Data Breach Response Plan. Review insurance coverage for data breaches and consider whether it needs to be updated in light of the higher fines and penalties under the GDPR. Review liability provisions in agreements for breaches caused by service providers and other partners. 	32-34
Data transfer	<ul style="list-style-type: none"> Identify all cross-border data flows and review data export mechanisms Update cross border mechanisms if necessary.. 	

Rights of data subjects under the GDPR

- Right to withdraw consent - Article 7
- Right to lodge a complaint - Article 13 (d)
- Right of access - Article 15
- Right to rectification - Article 16
- Right of erasure - Article 17
- Right to restrict **processing** - Article 18
- Right of portability - Article 20
- Right to object to **processing** - Article 21
- Rights in relation to automated **processing** - Article 22
- Right to an effective judicial remedy - Article 78
- Right to representation of **data subject** - Article 80
- Right to compensation - Article 82

Examples of data subject's rights: What needs to be done

Right to object to profiling

01. Conduct an analysis of all current profiling activities and determine which will require explicit consent (those profiling activities which use special categories of data and those profiling activities which are not necessary for a contract or required by law).
02. Implement or update privacy notices to refer to profiling activities. These will need to be tailored to the particular profiling in order to specify any likely effect on the **data subject**.

Right of Data Portability

01. Review personal data on systems to establish how they can be provided to the **data subject** and third parties on request.
02. Review systems to ensure that these enable the deletion of personal data that is no longer required.
03. Establish policies and procedures for responding to requests from **data subjects**.

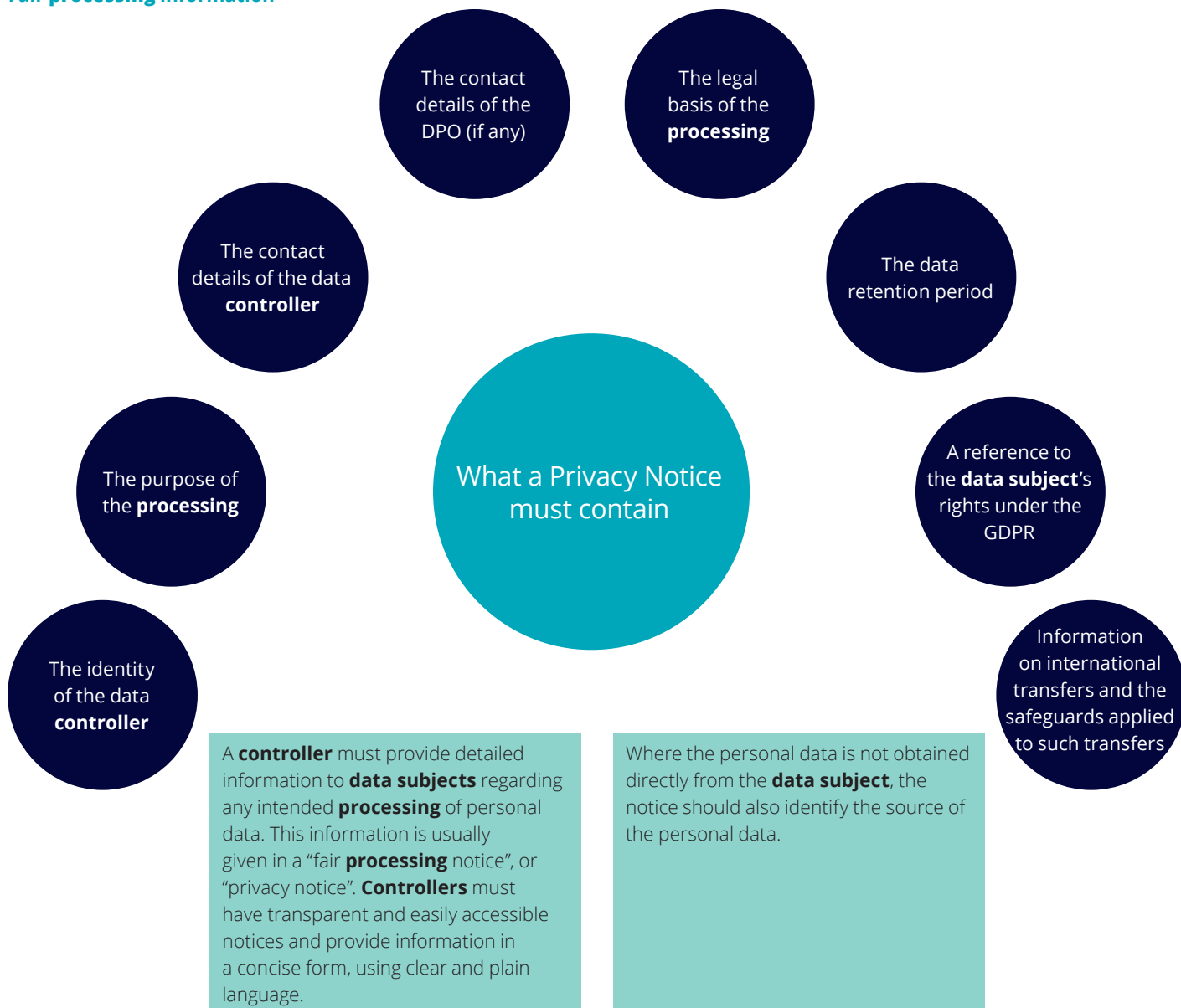
Right of Erasure

01. A data retention policy should be implemented to define the legal and regulatory reasons for retaining categories of personal data for specified periods of time. This policy needs to be implemented into both new and existing systems.
02. Policies and procedures should be put in place documenting how erasure requests are to be handled.
03. Prioritise transition of personal data from historic systems onto new systems which can be built to incorporate data retention and destruction rules.





















Access, Notification, and Restriction, and Direct Marketing

01. Implement subject access request policies and procedures.
02. Develop new policies for prompt rectification of personal data and a procedure to cease **processing** where applicable.
03. Implement a policy for dealing with marketing objections and maintain a suppression list.

Fair processing information



The Right to be Informed: Articles 12(1), 12(5), 12(7), 13, and 14

What information must be supplied	Data obtained directly from data subject	GDPR Articles
Identity and contact details of the controller and where applicable, the controller's representative) and the DPO		
Purpose of the processing and the legal basis for the processing		
The legitimate interests of the controller or third party, where applicable		
Any recipient or categories of recipients of the personal data		
Details of transfers to third country and safeguards		
Retention period or criteria used to determine the retention period		
The existence of each of data subject's rights		
The right to withdraw consent at any time, where relevant		
The right to lodge a complaint with the IDPC		
The source the personal data originates from and whether it came from publicly accessible sources		
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data		
The existence of automated decision making, including profiling, and information about how decisions are made, the significance, and the consequences.		
When should information be provided?	At the time data is obtained	Within a reasonable period from when data is obtained
		At the latest with first communication is made
		If disclosure to another recipient envisaged, at the latest before disclosure is made

GDPR obligations

Obligations placed on processors

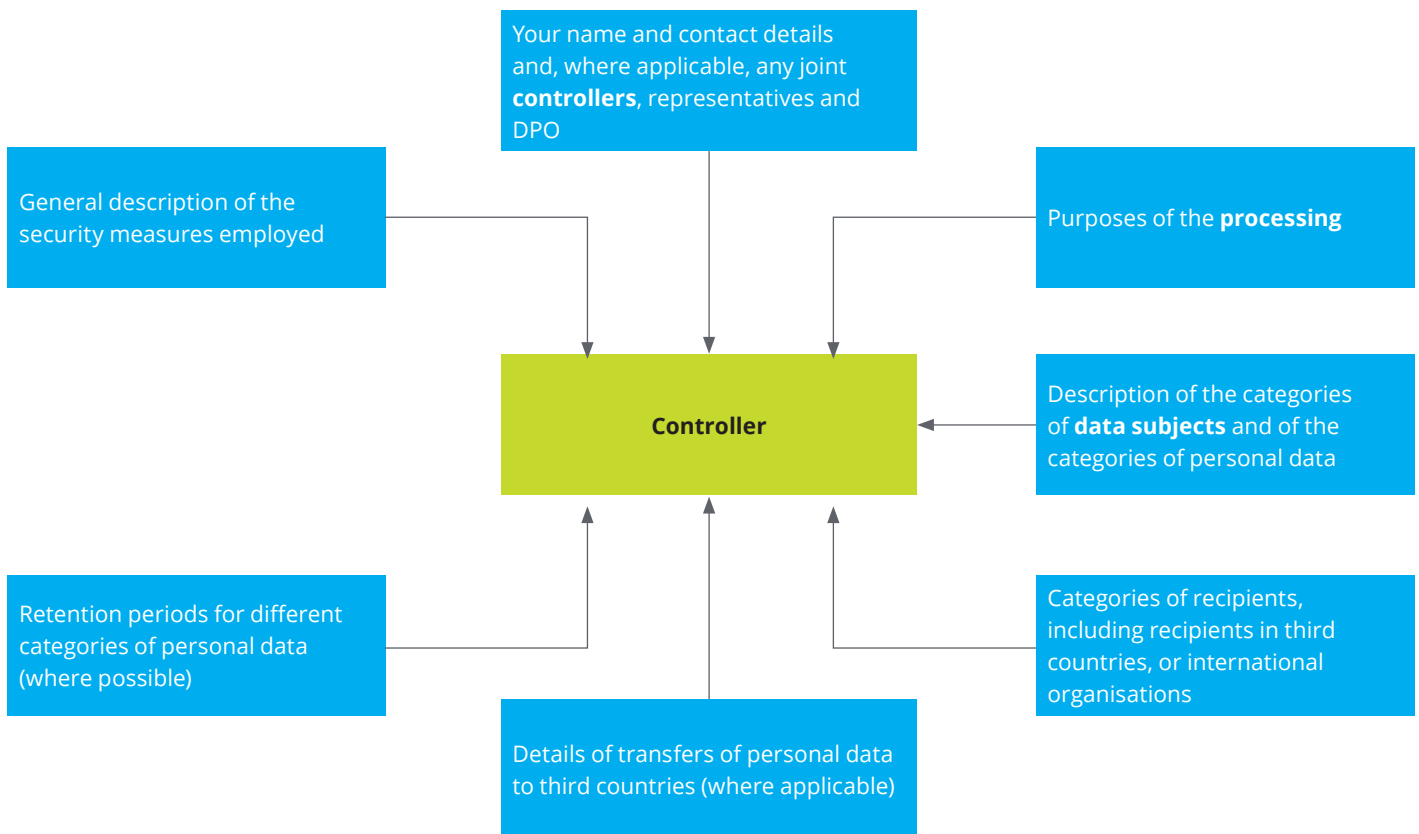
- Appoint a representative if based outside of the EU : **Article 27**
- Ensure certain minimum provisions in contracts with **controllers**. **Article 28(3)**
- Do not appoint sub-**processors** without specific or general authorisation of the **controller** and to ensure that there is a contract with the sub-**processor** containing certain minimum provisions. **Article 28(2) and (4)**
- Process personal data only on the instructions of the **controller** unless required to process for other purposes by EU or MS law. This will be a major headache for many foreign **processors**. **Article 29**
- Keep a record of **processing** carried out on behalf of **controller**. **Article 30**
- Cooperate with the IDPC. **Article 31**
- Implement appropriate security measures. **Article 32**
- Notify the **controller** of any personal data breach without undue delay. **Article 33**
- Appoint a DPO in certain cases. **Article 37**
- Comply with the rules on transfers of personal data outside of the EU. **Article 34**

Mandatory obligations for processor contracts

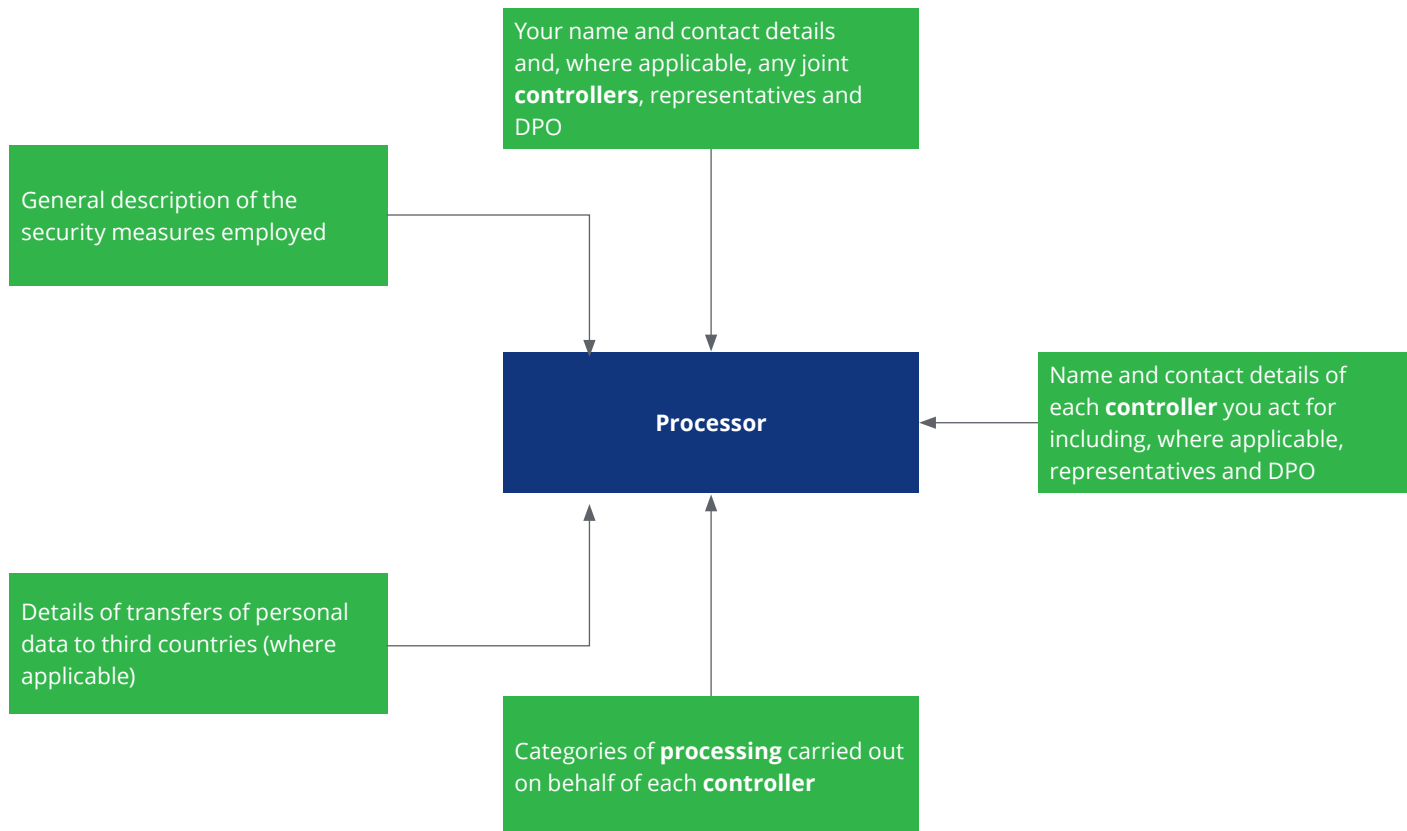
- The contract must contain a description of (i) scope, nature, and purpose of **processing**; (ii) duration of the **processing**; and (iii) types of personal data and categories of **data subjects**. **Article 28(3)**
- The **processor** may only process personal data on the documented instructions of the **controller**, including as regards international transfers. There is an exception for obligations under EU or MS law, but the **processor** must inform the **controller**. **Article 28(3)(a) Recital 81**
- The personnel used by the **processor** are under a statutory obligation of confidentiality. **Article 28(3)(b)**
- The **processor** must keep the personal data secure. **Article 28(3)(c)**
- The **processor** may only use a sub-**processor** with the consent of the **controller**. That consent may be specific to a particular sub-**processor** or general. Where the consent is general, the **processor** must inform the **controller** of changes and give them a chance to object. **Article 28(2) and Article 28(3)(d)**
- The **processor** must ensure it flows down these obligations to any sub-**processor**. The **processor** remains responsible for any **processing** by the sub-**processor**. **Article 28(4)**

- The **processor** must assist the **controller** to comply with requests from individuals exercising their rights to access, rectify, erase, or object to the **processing** of their personal data. **Article 23(3)**
- The **processor** must assist the **controller** with their security and data breach obligations, including notifying the **controller** of any personal data breach. **Article 28(3)(f) and Art. 33(2)**
- The **processor** must assist the **controller** should the **controller** need to carry out a privacy impact assessment. **Article 28(3)(f)**
- The **processor** must return or delete personal data at the end of the agreement, save to the extent the **processor** must keep a copy of the personal data under EU or MS law. **Article 28(3)(g)**
- The **processor** must demonstrate its compliance with these obligations and submit to audits by the **controller** (or by a third party mandated by the **controller**). Some **processors** will want to agree a “mandated” third party auditor to allow their existing process of independent third party certification to continue. **Article 28(3)(h)**
- The **processor** must inform the **controller** if, in its opinion, the **controller**’s instructions would breach EU or MS law. **Article 28(3)**

Recording keeping obligations



Recording keeping obligations



Sensitive Information

Sensitive personal data has been expanded to also include:



Gender identity



Trade union activities

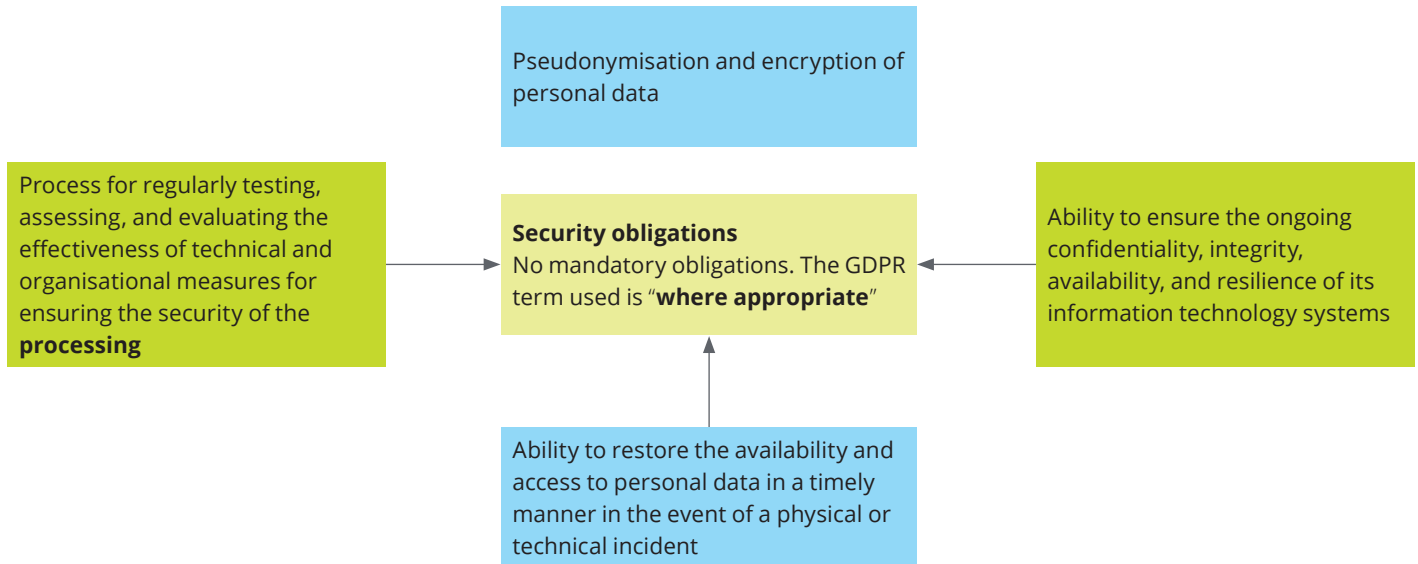


Administrative or criminal sanctions



Genetic or biometric data

Security obligations under the GDPR



Privacy by Design

Art. 25 (1) Privacy by Design

Implement technical and organisational measures at time of determination of the means of processing and at the time of processing itself.

Art. 25 (2) Privacy by Default

Only personal data which are necessary for each specific purpose are processed amount of data, the extent of their processing, storage period and accessibility .

01. Proactive not reactive—preventative not remedial.	Anticipate, identify, and prevent invasive events before they happen; this means taking action before the fact, not afterward
02. Lead with privacy as the default setting	Ensure personal data is automatically protected in all IT systems or business practices, with no added action required by any individual.
03. Embed privacy into design	Privacy measures should not be add-ons, but fully integrated components of the system.
04. Retain full functionality (positive-sum, not zero-sum)	Privacy by Design employs a “win-win” approach to all legitimate system design goals; that is, both privacy and security are important, and no unnecessary trade-offs need to be made to achieve both.
05. Ensure end-to-end security	Data lifecycle security means all data should be securely retained as needed and destroyed when no longer needed.
06. Maintain visibility and transparency—keep it open	Assure stakeholders that business practices and technologies are operating according to objectives and subject to independent verification.
07. Respect user privacy—keep it user-centric	Keep things user-centric; individual privacy interests must be supported by strong privacy defaults, appropriate notice, and user-friendly options.

Privacy By Design means building privacy into the design, operation, and management of a given system, business process, or design specification; it is based on adherence with the seven Foundational Principles of Privacy by Design.

Privacy by Design is a framework based on proactively embedding privacy into the design and operation of IT systems, networked infrastructure, and business practices.

Need for a pragmatic, holistic approach Protect yourself from common pitfalls



Data protection principles

- Accountability
- Storage limitation
- Purpose limitation
- Lawfulness
- Data minimisation



Strategy and processes

- Limited or no formal accountability
- Incident/breach management



Data Subject Rights

- Transparency
- Handling requests
- Automated decision-making and profiling



Data Governance

- Risk methodology
- Third party management
- Privacy
- Impact assessments

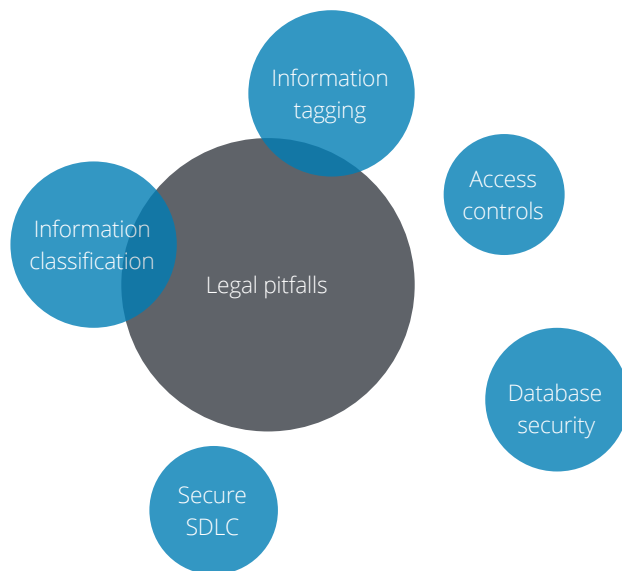
Privacy by Design/by Default

- Roles and responsibilities
- Audits
- International transfers
- Training and awareness



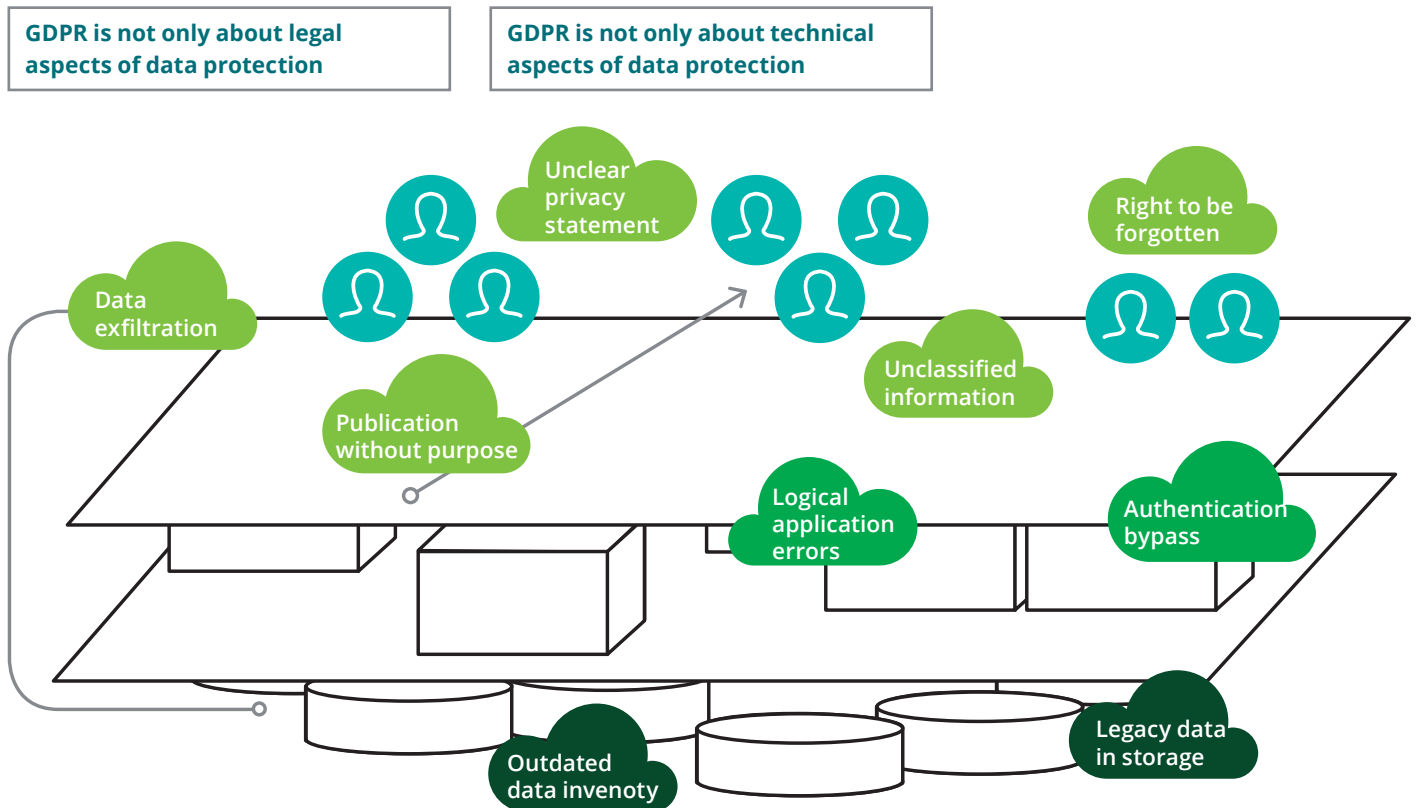
Technology

- Documentation
- Heterogeneous approach
- Lack of coordination and oversight

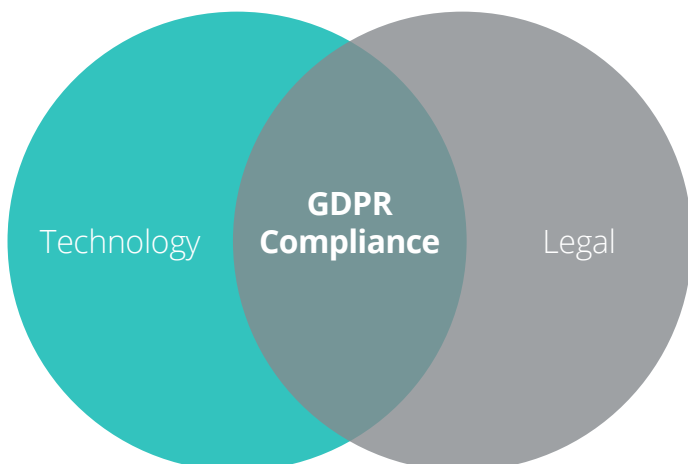


Design by Privacy: Software developers view on design

GDPR related challenges in your landscape



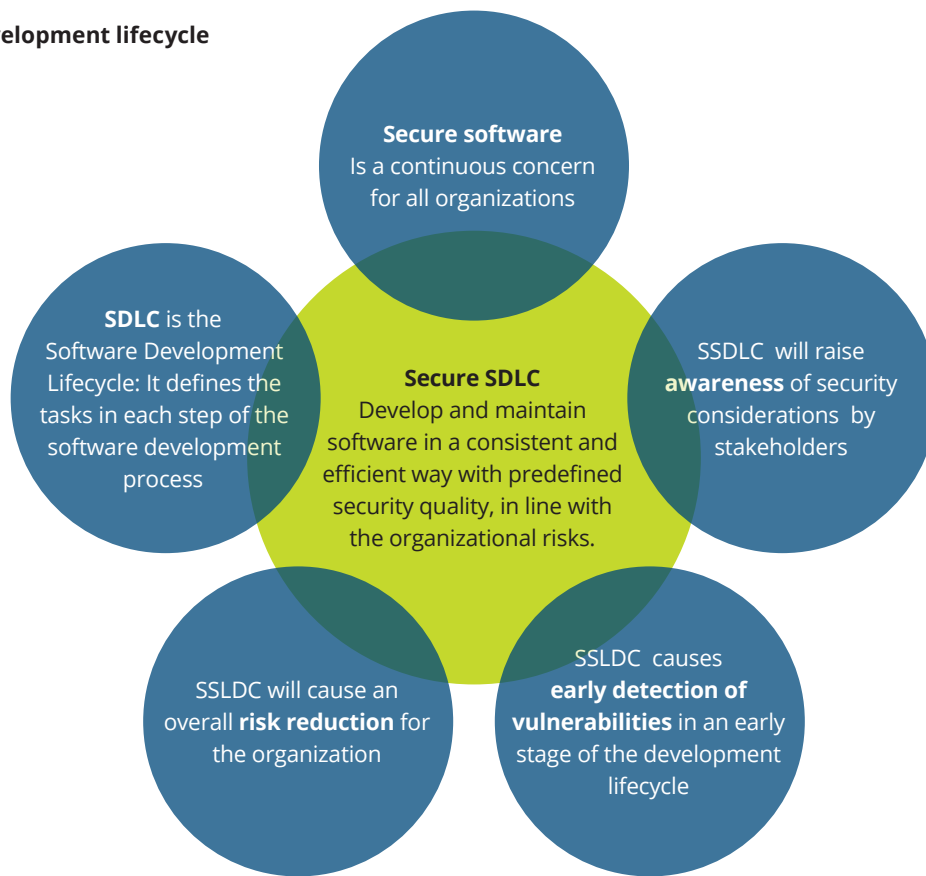
GDPR calls for a combined approach



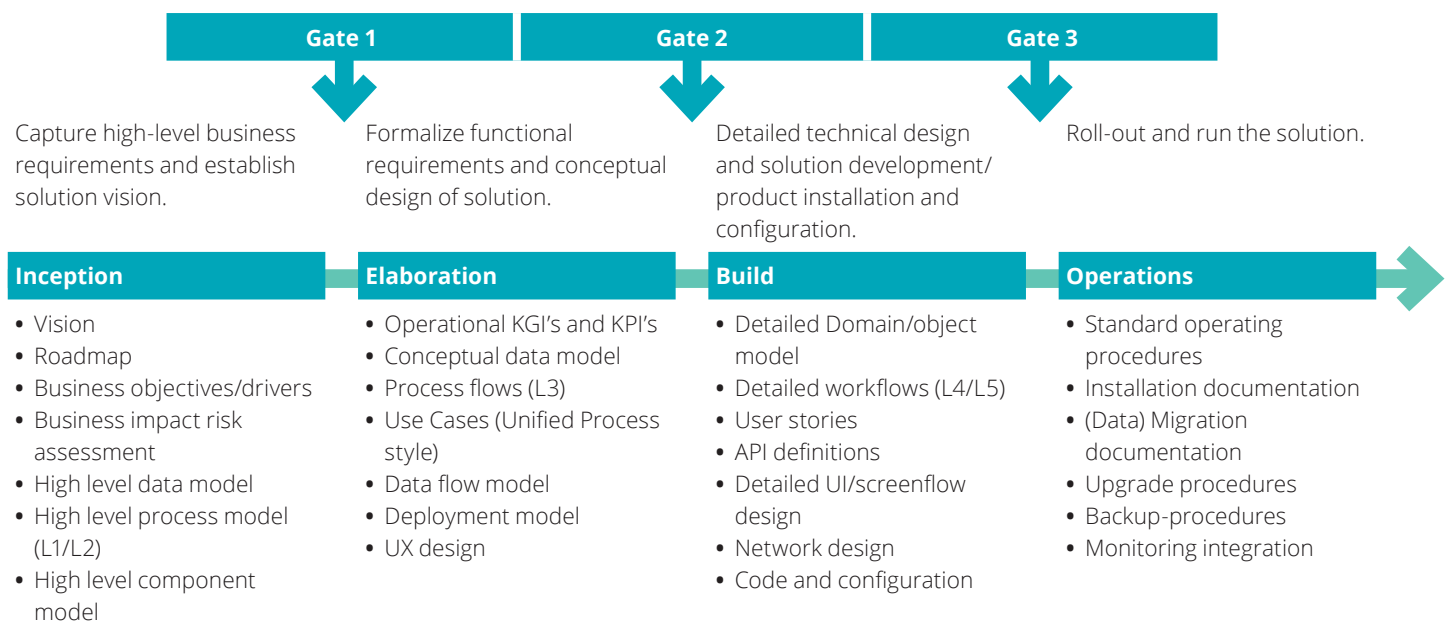
GDPR calls for a combined approach

Governance, organisation and people	<ul style="list-style-type: none"> Legal framework Privacy statements Roles and responsibilities 	Vision
Processes	<ul style="list-style-type: none"> Data lifecycle Management requirements gathering and privacy-aware processes 	Policies
Data	<ul style="list-style-type: none"> Information classification Information tagging Data (lifecycle) governance 	Procedures
Technology	<ul style="list-style-type: none"> Data(base) security Data leakage protection Data lifecycle management 	Instructions

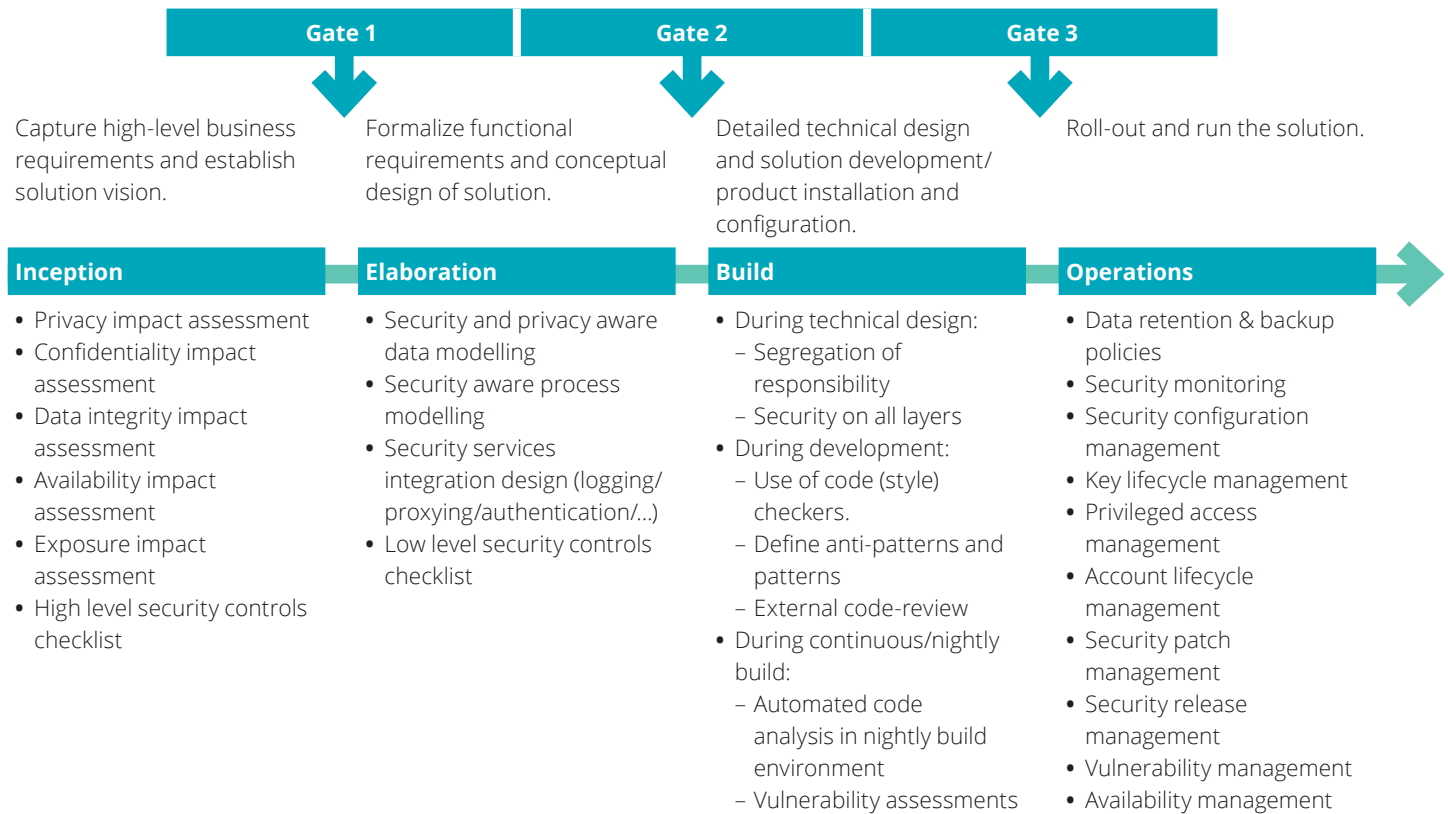
Secure software development lifecycle



Software development lifecycle deliverables



Software development lifecycle security and privacy control deliverables



Obligation to appoint a Data Protection Officer (DPO)

The Regulation now states that all public authorities will have to appoint a DPO.

In the private sector, companies that:



OR



OR



Process personal data of more than 5,000 individuals within a year

Are active in regular and systematic monitoring of individuals

Process data which is sensitive, location, relating to children, or employee data

will have the obligation to appoint a DPO.

Risk analysis and Data Protection Impact Assessments (DPIA)

There may now be an obligation to conduct a privacy risk analysis when setting up new business processes.

The personal data management lifecycle should be considered and focus on the controls that protect the accuracy, confidentiality, integrity, physical security and deletion of personal data.

Where the risk analysis indicates a high risk organisations will be obligated to conduct a DPIA.

While organisations' are not required to perform Privacy Impact Assessments (PIA), it is suggested that a risk analysis or PIA is performed.

One stop shop

1. Cross-border processing personal data

- Where an organisation has establishments in two countries; e.g. in Malta with a branch in Belgium.
- Where an organisation has an establishment in only one country but substantially effects data subjects in another country; e.g. established in Malta but targeting e-commerce for Belgians.

Processing that Substantially Affects

- Assessed on case by case basis taking account of (i) context of processing; (ii) type of data; (iii) purpose of processing; and (iv) factors such as damage, well-being, etc.

2. Lead supervisory authority

- Depends on determining the location of the controller's 'main establishment' or 'single establishment' in the EU – where main establishment means

Controller

- Place of its central administration.
- Unless the decisions on the purposes and means of the processing of personal data are taken in another establishment which has the power to implement such decisions.

Processor

- Place of its central administration in the EU.
- If processor has no central administration in the EU, the establishment of the processor in the EU where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under the GDPR

- Supervision of cross border processing should be led by only one supervisory authority (SA) in the EU: the lead SA will coordinate any investigation, involving other 'concerned' SAs.

3. Identifying lead supervisory for controller

- May be cases where an establishment other than the place of central administration makes autonomous decisions concerning the purposes and means of a specific processing activity – that is more than one lead SA can be identified.
- Companies are to identify precisely where the decisions on purpose and means of processing are taken. Criteria to be applied where main establishment is not the place of its central administration in the EU include:
 - Where are decisions about the purposes and means of the processing given final 'sign off'?
 - Where are decisions about business activities that involve data processing made?
 - Where does the power to have decisions implemented effectively lie?
 - Where is the director with overall management responsibility for the cross border processing located?
 - Where is the controller or processor registered as a company, if in a single territory?

4. Identifying lead supervisory involving both controller and processor

- Competent lead supervisory authority should be the lead supervisory authority for the controller.
- Supervisory authority of the processor will be a 'supervisory authority concerned' and should participate in the cooperation procedure.

- Supervisory authority of the processor will be a 'supervisory authority concerned' and should participate in the cooperation procedure.
- This rule applies only where the controller is established in the EU.
- A processor may provide services to multiple controllers located in different MS – e.g. a large cloud-service provider. Lead SA will be the SA that is competent to act as lead for the controller – may result in controller dealing with multiple SAs.

Extra-territorial effect

When assessing if a business established outside of Europe offers goods or services to **data subjects** in Europe, consideration is to be given to whether the business is:

- Offering services in a language or currency of an MS;
- Enabling European residents to place orders in such other language;
- Referencing European customers in its publications.

If one or more of these conditions are present, this may make it “apparent that the data **controller** envisages offering goods or services” to European residents and it is likely to be considered to be subject to the GDPR.

A large number of businesses previously operating outside the scope of 45\96\EC or MS data protection legislation will now be caught by the GDPR and therefore they should assess whether their activities will bring them within the scope of the GDPR. Some examples are presented opposite.

Situation	Caught by the DPA 2001 [CAP440]	Caught by GDPR?
US social media company with no European presence, targeting the Service at individuals in Europe	No	Yes
Chinese e-commerce retailer with website in English, accessible by European citizen, but does not provide delivery to EU MS	No	No
Chinese e-commerce retailer with website in English, accessible by European citizen, and allows E-purchase by citizens of EU MS	No	Yes
Japanese website uses cookies which monitors behaviour and sends targeted marketing to IP addresses, which include those from citizens of EU MS	No	Yes

Sanctions



€10 million, or 2% of worldwide annual turnover in preceding FY in case of an undertaking (whichever is the greater).



€20 million, or 4% of worldwide annual turnover in preceding FY in case of an undertaking (whichever is the greater).

Relevant articles

- **8.** Child's consent
- **11. Processing** not requiring identification
- **25.** Data protection by design and by default
- **26.** Joint **controllers**
- **27.** Representatives of **controllers/processors** not established in the EU
- **28-30 and 32. Processing**
- **31.** Co-operation with the IDPC
- **33.** Notification of breaches to the IDPC
- **34.** Communication of breaches to **data subjects**
- **35.** DPIA
- **36.** Prior consultation
- **37-39.** DPOs
- **41(4).** Monitoring of approved codes of conduct
- **42 and 43.** Certification

Relevant articles

- **5.** Principles for **processing** personal data
- **6.** Lawfulness of **processing**
- **7.** Conditions for consent
- **Processing** special categories of personal data
- **12-22 Data subject's** rights (information, access, rectification, etc.)
- **40-50** Transfer to third countries
- **58(1)** Requirements to provide access to the IDPC
- **58(2)(f)** and **58(2)(g)** and **58(2)(j)**: Orders/Limitations on **processing** or the suspension of data flows
- Obligations adopted under MS law

EU-US Privacy shield will now replace Safe Harbor

What will change?

New framework will:

- Move away from a self-regulatory approach with increased oversight, enforcement, and sanctions
- Increase role of European national data protection authorities

Main headlines:

- Strong obligations on companies – enforceable under U.S. law and will have to commit to comply with decisions by European DPAs.
- Clear safeguards and transparency obligations on U.S. government access – no mass surveillance on the personal data transferred to the US under the new arrangement
- Effective protection of EU citizens' rights – several redress possibilities for citizens including a new Ombudsperson.

What have other organisations been doing?

- Many companies have been implementing Model Contract Clauses for both internal
- data transfers and agreements with data processors
- Cloud operators increasing data center locations in Europe



Frequently asked questions



My business operates in Italy as well. Do I still have to get advice on how the GDPR is implemented in Italy?

It depends on what **processing** you carry out. There still are national variations in some areas, which will require review under Italian law. One example is **processing** of information about employees: MS can introduce additional protections for employees. There is also overlap with national labour laws and there may be differences in the way the rules are interpreted and enforced. The differences will narrow over time, and the GDPR contains a consistency mechanism to help do that.

As I operate in Malta and Italy do I need to nominate a supervisory authority?

Given that you operate from both Malta and Italy the lead supervisor will be the competent authority where you have the 'main establishment' located. The 'main establishment' is determined by considering where the central administration is, where the decisions on **processing** personal data are taken, and where the main **processing** activities take place. If the main establishment is located in Malta then the lead supervisory authority is the IDPC in Malta.

Does the 'one stop shop' mean I am just subject to the supervision of my home regulator?

If you carry out cross border **processing**, you will be primarily regulated by supervisory authority based in the jurisdiction of your main establishment. The "one stop shop" does not apply where **processing** is based on the legal obligation or public function condition and other supervisory authorities can ask to take control where the **processing** mainly relates to their jurisdiction. The lead supervisory authority can refuse to cede control, but must co-ordinate its activities closely with other 'concerned' supervisory authorities.

Has the GDPR changed at all from the DPA 2001 (CAP 440)?

The core rules are broadly the same. The GDPR looks familiar to experienced privacy practitioners. This does not mean that there is no change. Rather, there are some significant changes. The GDPR adds a number of important new obligations. Finally, there is a significant increase in the sanctions for getting it wrong.

Do I have to get consent from an individual?

Not necessarily. Consent is only one of a number of justifications for **processing** the individual's personal data. Other justifications, such as the so-called legitimate interests condition, are available.

What happens if someone withdraws consent?

It is likely that you will have to stop **processing** that individual's personal data, although in some cases you may be able to rely on an alternative **processing** condition. Withdrawal of consent may also give the individual the right to be forgotten, i.e. have their data erased. Withdrawal of consent does not affect the lawfulness of any **processing** that takes place prior to that withdrawal.

A customer has asked to be "forgotten" and for all his data to be deleted. Do I have to comply?

It depends. Assuming the customer is an individual, they do have a right to be forgotten but that right is not absolute. In particular, you would need to confirm a range of issues such as whether you were just relying on consent to process his or her data and whether you have a continuing need to hold the relevant personal data. In some cases, you may need to quarantine his or her personal data rather than delete it. The position is complex. You need to put a process in place to manage these requests.

What does the right to portability mean?

Individuals already have a right to access their personal data through a subject access request. The data portability enhances this right, giving the individual the right to get that personal data in a machine readable format. Individuals can also ask for the data to be transferred directly from one **controller** to another. There is no right to charge fees for this service.

The right only applies:

- To personal data "provided to" the **controller**. This will clearly apply to photos posted to a social network or content stored on a cloud service.
- Where the **controller** is **processing** personal data in reliance on the **processing** conditions of consent or performance of a contract.

Is consent given under the DPA 2001 (CAP440) still valid?

Where consent is given under the DPA2001 (CAP440), it will continue to be valid under the GDPR if it also meets the requirements of the GDPR.

Will the definition of consent under the ePrivacy Directive remain the same?

The ePrivacy Directive currently defines consent by reference to the 45/96/EC Directive. This will automatically be superseded by a reference to the GDPR from May 2018 onwards. In other words, obtaining consent to market by email will become a whole lot harder as well.

The need for consent doesn't just arise from the GDPR but also in a number of other laws. Will this result in confusion?

Correct. If you are subject to bank secrecy laws, it is very likely you will need consent to disclose customer information. You may find that you ask for, and obtain, a valid consent for the purposes of bank secrecy laws, but that consent is not valid for data protection purposes (e.g. because it is tied to performance of the banking contract). You must, therefore, make it clear which **processing** condition you are relying

Can a customer object to direct marketing?

When an individual exercises the right to object to direct marketing, you must not only stop sending direct marketing material to the individual, but also stop any **processing** of that individual's personal data for such marketing. For example, if you receive an objection, you should stop profiling that individual to the extent related to direct marketing. The ePrivacy Directive contains additional restrictions on marketing and in some cases requires the consent of the individual. The ePrivacy Directive will continue to apply in parallel with the GDPR.

Our school sends and requests coursework from its primary and secondary students on line – which means all students must have access to email and the Internet?

The SDPR contains specific protections for children. You can only get consent from a child in relation to online services if it is authorised by a parent. A child is someone below the age of 16, though MS can reduce this age to 13 years.

The GDPR does not apply this restriction when obtaining consent from a child offline, but given the tight controls on consent, you may still wish to obtain parental authorisation.

The GDPR adds:

- Privacy policies must be very clear and simple if they are aimed at children.
- Profiling and automated decision making is not to be applied to children.
- The right to be forgotten applies very strongly to children.

Is the right not to be subject to profiling and automated decision making a blanket one?

An customer has the right not to be subject to decisions made automatically that produce legal effects or significantly affect him / her. This right, however, does not apply where the decision is:

- Based on explicit consent from the individual, subject to suitable safeguards including a right for a human review of the decision.
- Necessary for a contract, subject to suitable safeguards including a right for a human review of the decision.
- Authorised by EU or MS law.

What policies do I need?

It depends on your business. You would expect a large business to have a general data protection policy and policies that address the data protection issues arising out of marketing, data security, recruitment, record retention and monitoring. These do not have to be stand-alone policies and the data protection issues might be built into a wider policy.

How can I “demonstrate” I am complying with the GDPR?

You will need to update or create suitable policies that set out how you process personal data. You should also consider other compliance measures, including setting up a clear compliance structure, allocating responsibility for compliance, staff training, and audit. It might also involve technical measures such as minimising **processing** of personal data, pseudonymisation, giving individuals greater control and visibility, and applying suitable security measures.

Is it mandatory to appoint a DPO?

The GDPR establishes the appointment of a DPO if:

- You are a public authority – a government entity, authority, or body other than a court.
- Your core activities consist of regular and systematic monitoring of data on a large scale.
- Your core activities consist of **processing** sensitive personal data on a large scale (including criminal offences).

The national MS law may establish the appointment of a DPO as mandatory. No such notice has been given to data by the IDPC.

What is the role of the DPO?

The DPO is a means to ensure accountability and compliance with the GDPR without external intervention by the IDPC. The DPO monitors compliance, provides information and advice, and liaise with the IDPC. The DPO must report to the highest level of management within your business. The DPO must be able to operate independently and not be dismissed or penalised for performing their tasks.

Should the DPO form part or lead a company's privacy compliance function?

The DPO is responsible for monitoring compliance with the GDPR, providing information and advice, and liaising with the IDPC. There are good arguments for the DPO to be separate from the compliance unit and instead operates as a form of third line of defence. This avoids the risk of the DPO “marking their own homework”.

A person must be qualified to assume the role of DPO and if so what qualification should s/he hold?

The DPO must have the right professional qualities and expert knowledge of data protection law. There is no express requirement for them to hold any particular qualification or certification. However, obtaining appropriate qualifications will be an effective way to demonstrate expert knowledge (and may help them to do their job properly).

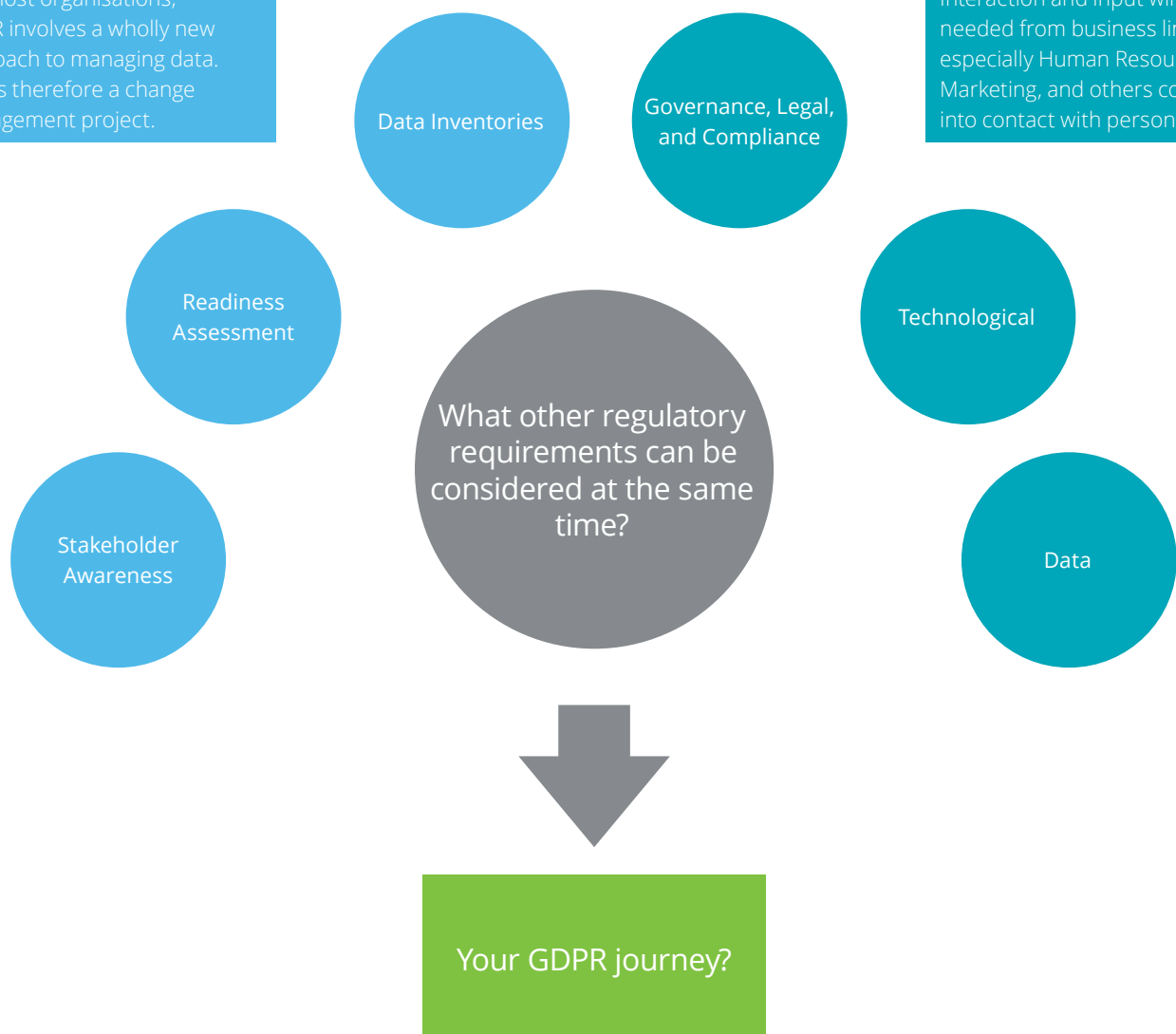
Does the breach notification obligation relate to the obligations in the Cyber Security Directive?

The obligations in the GDPR apply in parallel with those in the Network and Information Security Directive and the ePrivacy Directive.

Managing your GDPR project

For most organisations, GDPR involves a wholly new approach to managing data. This is therefore a change management project.

Interaction and input will be needed from business lines especially Human Resources, Marketing, and others coming into contact with personal data



Deloitte's approach: Compliant, yet innovative

Today's business climate is characterised by disruption and volatility. At Deloitte, we help businesses gain a new view of risk—seeing risk management as a vital performance lever, revealing untapped opportunities to create competitive advantage.

There are lines you cannot cross. There are rules to the game. But within the lines and following the rules, you are only limited by your own creativity to achieve your goals.

We are dedicated to help organisations navigate privacy risk, staying within the rules of the game, while allowing privacy to be a business enabler and to use personal data to increase customer trust.

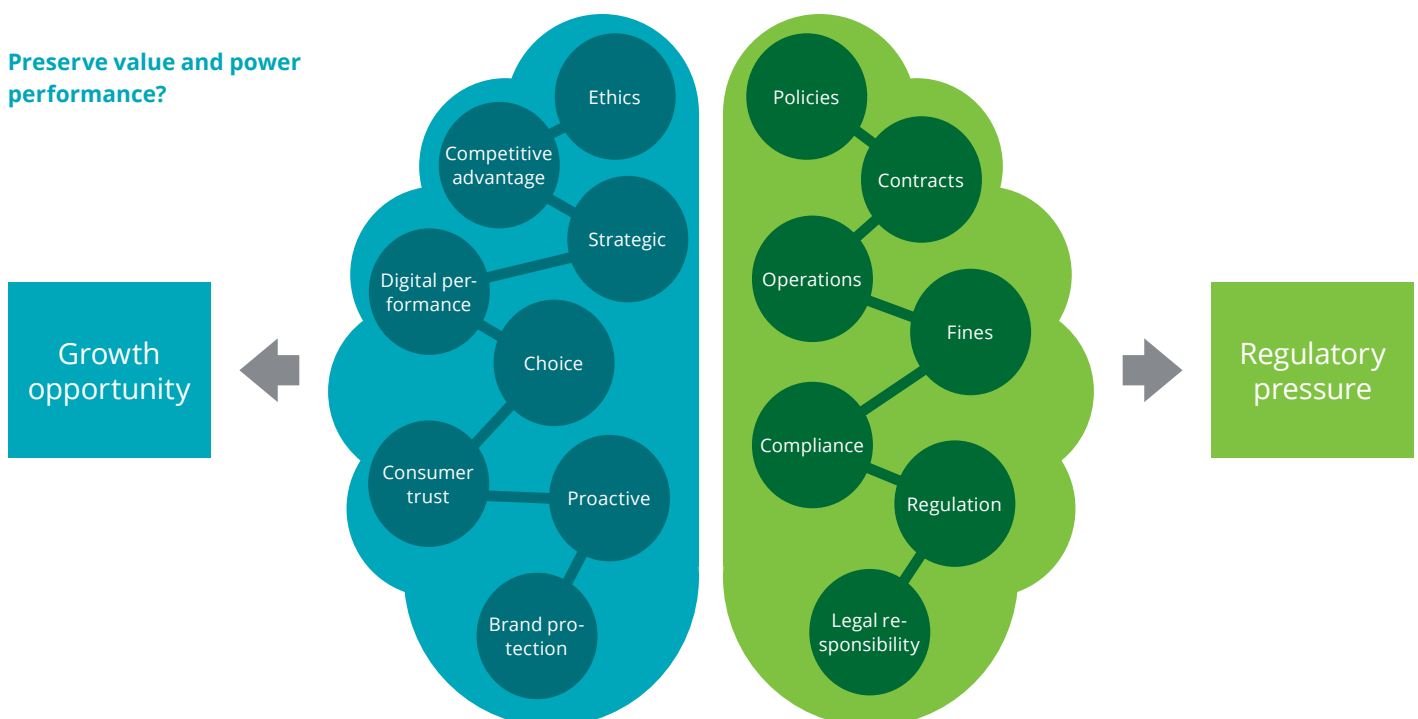
Our point of view on critical elements of the GDPR

When GDPR comes into effect on 25 May 2018 the European privacy landscape will be transformed which will mean a number of changes for organisations. We outline some major points from our experience that can help organisations getting the most from these changes.

01. Proper data management is essential to comply with the GDPR.
02. GDPR compliance will help build trust with clients and safeguard personal data.
03. Make GDPR compliance your top priority for the coming months.

Following these principles will greatly help you getting the most value from **processing** personal data, while minimizing the risk.

Preserve value and power performance?



Service offerings to help you prepare for the GDPR

GDPR Framework Programme Modules 1 - 9

- **Module 1:**
Quick Scan Assessment
- **Module 2:**
Governance and Accountability
- **Module 3:**
Detailed Gap Analysis
- **Module 4:**
Policies and Procedures
- **Module 5:**
Contracts With **processors** and third parties
- **Module 6:**
Data and Security
- **Module 7:**
Data Life cycle Mapping and Process Documenting
- **Module 8:**
Data Privacy Impact Assessment
- **Module 9:**
Stress Testing

Why Deloitte?

- We have a wide range of services geared towards protecting privacy and our clients' interests.
- We have a wealth of experience servicing clients in multiple industries.
- We are independent and provide objective guidance, support and training.
- We will help you to embed consistent, capable, objective across the business.
- In order to address privacy challenges correctly, these three focus areas: technical, legal and organisational, in your organisation need to be involved. Our team consists of experts on each of those fields.
- We provide real-world expertise that reflects our proven practices in data and privacy with some of the world's leading organisations.
- We serve our clients with quality and distinction, making a measurable and attributable impact.

Learn more

To learn more about how your organisation can successfully implement GDPR, please contact:



Ian Coppini

Leader - Risk Advisory

+356 2343 2000

icoppini@deloitte.com.mt

www.deloitte.com/mt/gdpr



Deloitte refers to one or more of Deloitte Touché Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte Malta refers to a civil partnership, constituted between limited liability companies, and its affiliated operating entities: Deloitte Services Limited, Deloitte Technology Solutions Limited, Deloitte Digital and Technology Limited, Alert Communications Limited, Deloitte Technology Limited, and Deloitte Audit Limited. The latter is authorised to provide audit services in Malta in terms of the Accountancy Profession Act. A list of the corporate partners, as well as the principals authorised to sign reports on behalf of the firm, is available at www.deloitte.com/mt/about.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte’s over 260,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

© 2018. For information, contact Deloitte Malta.