GDPR – Context, Principles, Implementation, Operation, Data Governance, Data Ethics and Impact on Outsourcing

Úna Tighe BL
Law Library
una@unatighe.com

Alan McSweeney
https://www.linkedin.com/in/alanmcsweeney/

Contents

1. Introduction

You will by now have attended multiple presentations and other sessions of the subject of GDPR. You will have been offered GDPR-related services by many individuals, organisations and service providers.

There is a vast amount of material widely and readily available on GDPR. I do not intend to repeat this material here. I have included links to what I believe is some of the more useful and relevant information. It is very late to be giving specific advice on being compliant with GDPR given that it is becoming operational in two months. For that reason, I do not intend to do this here.

The overwhelming volume of material available on GDPR combined with vagueness and uncertainty around its interpretation and its actual implementation and operation and a lack of statements on or direction about actual requirements or practical advice or a definitive explanation has combined to create a certain paralysis.

In Ireland, the Data Protection Bill 2018 which gives effect to the GDPR was only published on 30 January 2018:

https://www.oireachtas.ie/viewdoc.asp?DocID=37646
http://www.oireachtas.ie/documents/bills28/bills/2018/1018/b1018s.pdf
https://www.oireachtas.ie/documents/bills28/bills/2018/1018/b1018s-memo.pdf

The consulting company Garter have estimated that by the end of 2018 over 50% of organisations affected by the GDPR will not be in full compliance with it.

As legal firms you will face two separate sets of GDPR-related challenges:

- In being compliant in your own internal processes and systems – in reality this is the lesser of the two challenges

- In providing clients with a range of advice and services of how they can achieve compliance with GDPR and in addressing their general data protection concerns. The type of advice depends on the client – small business, provider of data services

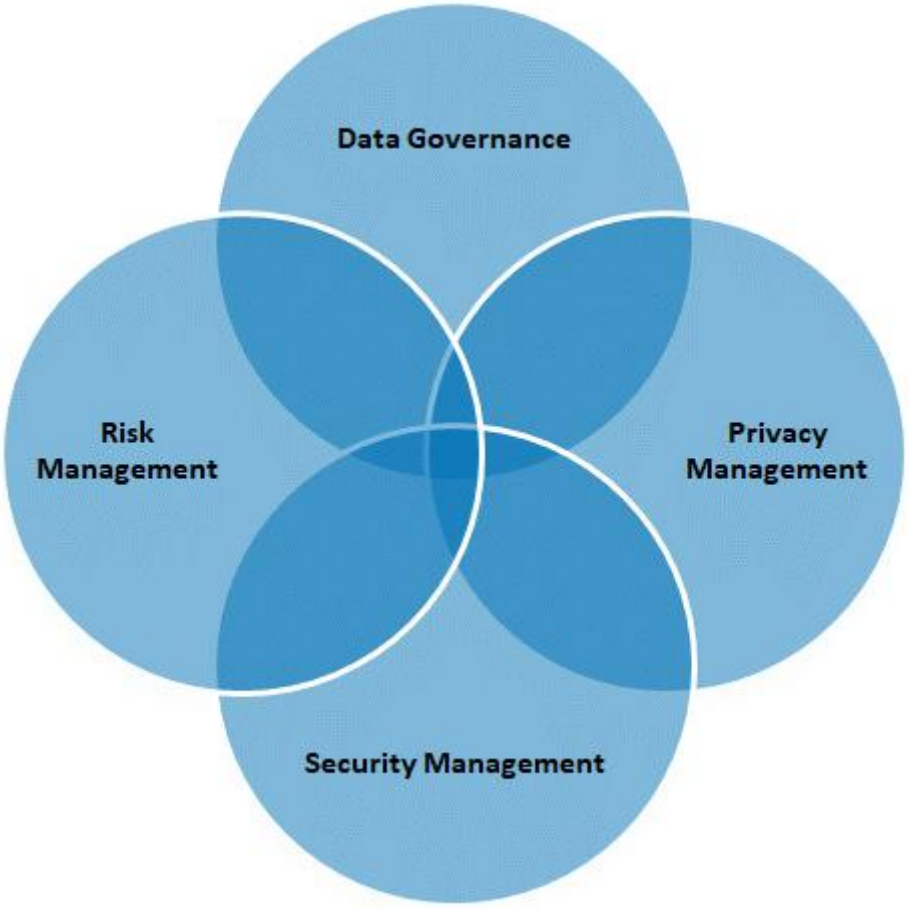
The objective of this session is to provide details on the context, implementation and operation of GDPR and related regulations and directives for organisations rather than repeating material you will undoubtedly already have seen. I have attempted to collate some of the more relevant material here.

I have taken a wider view of the data protection framework organisations need to implement and approaches they need to take.

GDPR and its related regulations have different impacts depending on the profile of your organisation and the way you collect and process information about individuals. There is no one solution to achieving GDPR compliance that applies to all organisations. However there are core principles.

GDPR impacts on the areas of:

- Data Governance
- Privacy Management
- Security Management
- Risk Management



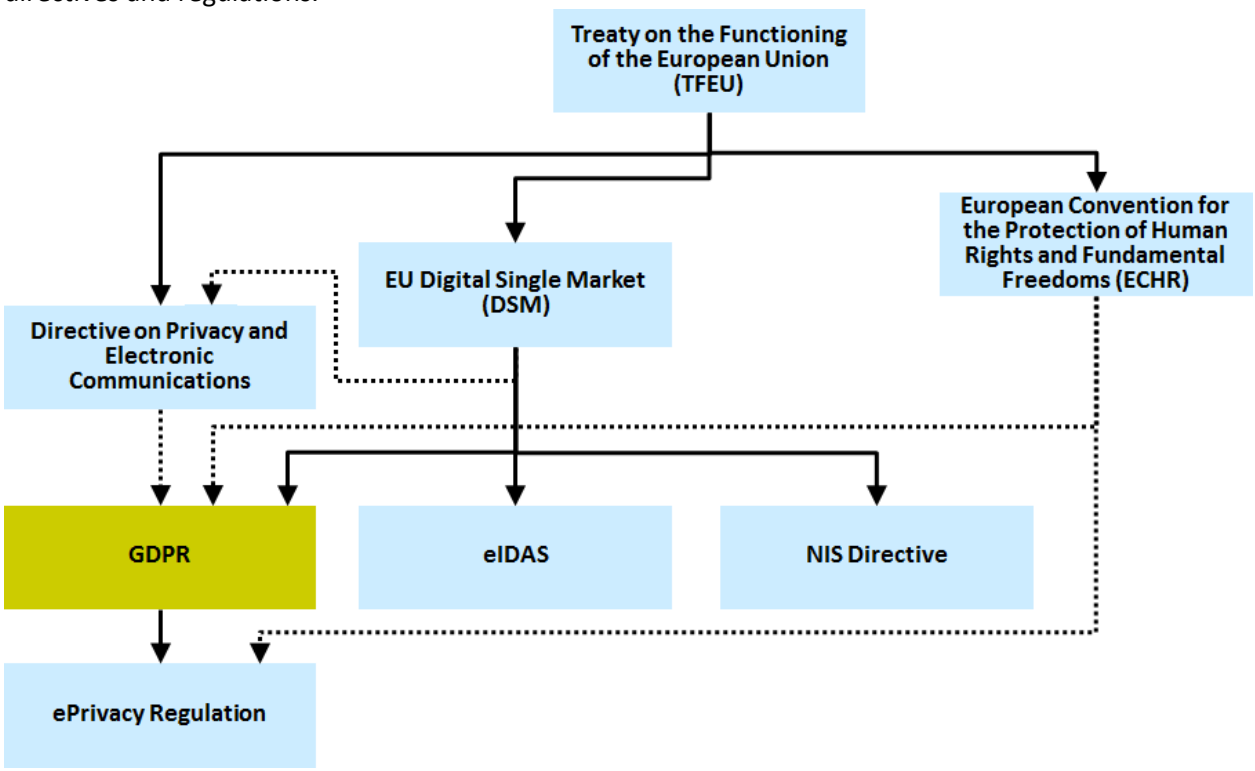
The topics I will cover here are:

- **Context of GDPR** – this contains information on other directives and regulations relating to GDPR to provide details on its wider content
- **Personal Information** – this reiterates what is meant by personal information and so what is covered by GDPR
- **Principles of GDPR** – this identifies some of the key principles that underpin GDPR and will affect its operation
- **Implementing and Operating GDPR** – this discusses approaches to operationalising GDPR within organisations
- **GDPR and Outsourcing** – this contains details on the particular topic of outsourcing that will be impacted by GDPR
- **Data Governance** – this puts GDPR into wider Data Governance context
- **Data Ethics** – this briefly discusses the wider issue of data ethics is the context of GDPR

2. Context of GDPR

The GDPR (http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679) exists within the context of the wider EU Digital Single Market (DSM) strategy and a related set of regulations and directives. Its objective is to increase trust in and the security of digital services in order to advance digital opportunities for citizens and businesses in Europe. It aims to strengthen the position of the EU as a digital economy world leader.

This representation of the wider context of GDPR is far from exhaustive. It just highlights the main other directives and regulations.



In this diagram, the dotted lines show indirect relationships.

This lists the main directives and regulations only. There are others such as:

- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045

Together these comprise a comprehensive set of regulations and standards. GDPR imposes rules on data processing that impacts almost all aspects of electronic or digital communications. The others have less impact in more narrowly focussed areas.

More details on the EU Digital Single Market are available from https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market.

The communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Digital Single Market Strategy for Europe is available from http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX%3A52015DC0192.

There are ambiguous objectives between these regulations regarding privacy and openness. On the one hand, the EU wants to impose regulations to protect personal data, its collection and use and on the other hand it wants to encourage new technology-based services and commerce. Regulations have a cost and impact the operation of business.

2.1 Directive on Security of Network and Information Systems (NIS Directive)

The text of the Directive on Security of Network and Information Systems (NIS Directive) is available from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC. This also comes into force on 25 May 2018, the same day as GDPR.

The aim of this directive is to ensure there is a common and high-level of EU-wide information systems and network security through a number of actions:

- Improving national information and network security capacity and effectiveness including having Computer Security Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs)

- Increasing co-operation on information and network security across all EU member states

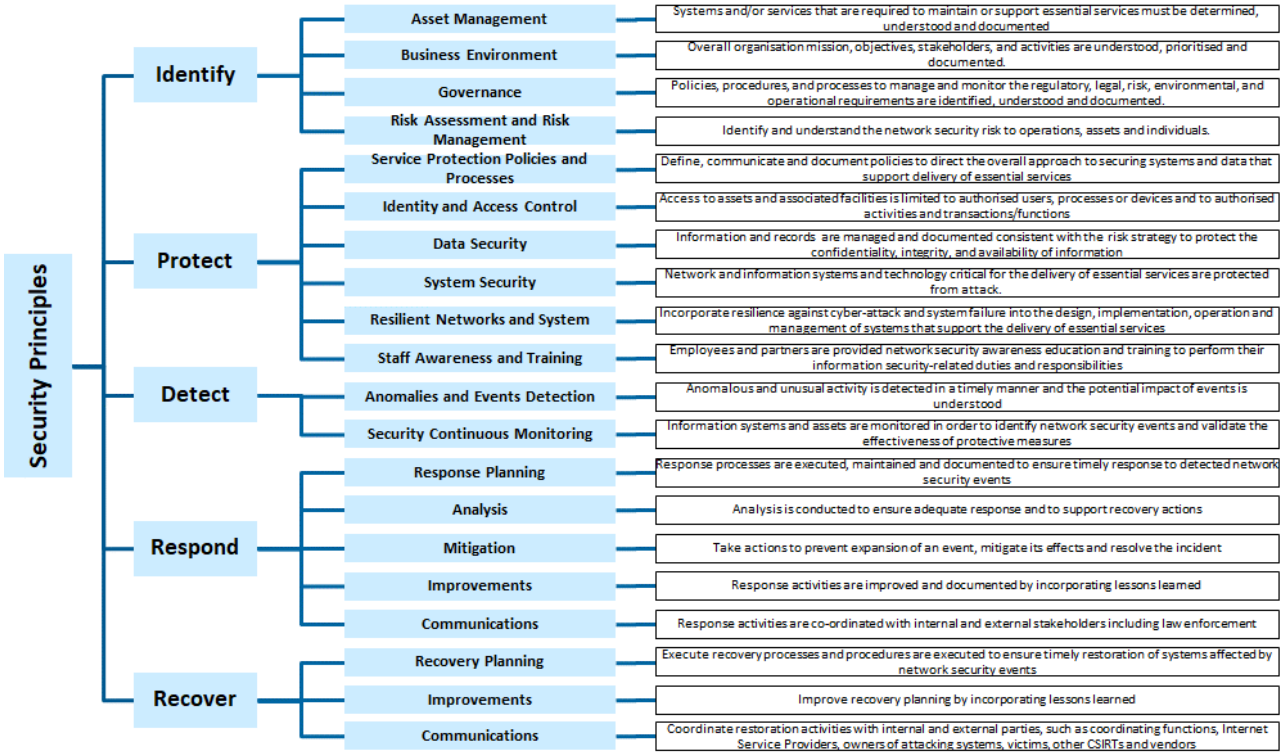
- Introducing binding security obligations and incident reporting obligations for operators of essential services (OESs) in critical national infrastructure (CNI). CNI providers include energy, healthcare, financial services, transport, drinking water supply, digital infrastructure and telecommunications services.

- States have to implement and operate a regulatory regime on digital service providers (DSPs). DSPs include providers of cloud computing services, online market places and search engines.

- States will be responsible for dealing with the security of services provided by multinational companies across the European Union that have their European headquarters located in that country.

The NIS Directive primarily applies to governments and state agencies responsible for critical infrastructure security, providers of critical infrastructure and digital service providers.

NIS primarily imposes obligations on member states. The states then impose obligations on different sets of service providers. NIS defines a set of security principles. While these do not apply to many organisations, the framework could be adopted by them as a check list to ensure their IT systems and processes are secure to meeting the security management requirements of GDPR.



The details of a security policy are:

Identify	**Asset Management**	Systems and/or services that are required to maintain or support essential services must be determined, understood and documented
	Business Environment	Overall organisation mission, objectives, stakeholders, and activities are understood, prioritised and documented.
	Governance	Policies, procedures, and processes to manage and monitor the regulatory, legal, risk, environmental, and operational requirements are identified, understood and documented.
	Risk Assessment and Risk Management	Identify and understand the network security risk to operations, assets and individuals
Protect	**Service Protection Policies and Processes**	Define, communicate and document policies to direct the overall approach to securing systems and data that support delivery of essential services
	Identity and Access Control	Access to assets and associated facilities is limited to authorised users, processes or devices and to authorised activities and transactions/functions
	Data Security	Information and records are managed and documented consistent with the risk strategy to protect the confidentiality, integrity, and availability of information
	System Security	Network and information systems and technology critical for the delivery of essential services are protected from attack
	Resilient Networks and System	Incorporate resilience against cyber-attack and system failure into the design, implementation, operation and management of systems that support the delivery of essential services
	Staff Awareness and Training	Employees and partners are provided network security awareness education and training to perform their information security-related duties and responsibilities
Detect	**Anomalies and Events Detection**	Anomalous and unusual activity is detected in a timely manner and the potential impact of events is understood

	Security Continuous Monitoring	Information systems and assets are monitored in order to identify network security events and validate the effectiveness of protective measures
Respond	**Response Planning**	Response processes are executed, maintained and documented to ensure timely response to detected network security events
	Analysis	Analysis is conducted to ensure adequate response and to support recovery actions
	Mitigation	Take actions to prevent expansion of an event, mitigate its effects and resolve the incident
	Improvements	Response activities are improved and documented by incorporating lessons learned
	Communications	Response activities are co-ordinated with internal and external stakeholders including law enforcement
Recover	**Recovery Planning**	Execute recovery processes and procedures are executed to ensure timely restoration of systems affected by network security events
	Improvements	Improve recovery planning by incorporating lessons learned
	Communications	Coordinate restoration activities with internal and external parties, such as coordinating functions, Internet Service Providers, owners of attacking systems, victims, other CSIRTs and vendors

2.2 ePrivacy Regulation

The ePrivacy Regulation (COM/2017/010) replaces the ePrivacy Directive (2002/58/EC (Regulation on Privacy and Electronic Communications).

The text of the regulation is available from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

The ePrivacy Regulation is a lex specialis of the GDPR. It extends GDPR by defining specific rules for the purposes of:

- Ensuring the protection of fundamental rights and freedoms, in particular the respect for private life, confidentiality of communications and the protection of personal data in the publicly available electronic communications sector in the EU
- Guaranteeing the free movement of electronic communications data, equipment and services in the EU

GDPR and the ePrivacy Regulation need to be considered together.

The scope of the ePrivacy Regulation includes:

- All people and businesses in the EU have the same level of protection of their electronic communications
- One set of rules will apply across the EU
- The enforcement of the rules will be the responsibility of the national data protection authorities
- Privacy rules will apply to newer providers of electronic communications services (termed Over-the-Top communications services (OTT)) such as Facebook Messenger, LinkedIn, Skype, WhatsApp and an increasing number of others ensuring that users of these services have the same level of confidentiality of communications as are provided by traditional telecoms operators

- Covers both communication content and metadata – information about content and the communication process: privacy is guaranteed for both content and metadata such as date and time of a communication, location, duration, end-points of a communication. Metadata is regarded as highly private. It is to be anonymised or deleted if users did not give their consent to its retention unless it is required for billing

- Browser cookie handling is changed. Browser settings have to provide an easy way to accept or refuse tracking cookies and other identifiers. This centralises consent for all web site accesses. No consent is needed for non-privacy intrusive cookies aimed at improving a user's experience (such as remembering a shopping cart history) or ones used to count the number of web site visitors

- Once consent is given for communications data - content and/or metadata - to be processed, there will be more opportunities to offer additional services

- Unsolicited electronic communications by email, text message and automated calling machines is banned. Marketers have to display their telephone number or use a pre-fix that indicates a marketing call. Depending on national law, people will either be protected by default or be able to use a do-not-call list in order not receive marketing phone calls

2.3 Directive on Privacy and Electronic Communications

This is Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1442330108842&uri=CELEX:32002L0058.

The GDPR refers to the Directive on Privacy and Electronic Communications in a number of locations:

> **Recital 173**
>
> This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation.
>
> **Article 21**
>
> Right to object
>
> 5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.
>
> **Article 95**
>
> Relationship with Directive 2002/58/EC

> This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

2.4 eIDAS (electronic IDentification, Authentication and trust Services)

This is regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Electronic Signatures Directive).

The text of the regulation is available from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.

It came into effect on 23 July 2014 and repealed directive 1999/93/EC with effect from 30 June 2016.

eIDAS defines a set of standards for electronic identification and trust services for electronic transactions in the European Single Market. It focuses on two areas:

- **Interoperability** – Member states are required to create a common framework that will recognise electronic Identifications (eIDs) from other member states and ensuring their authenticity and security.

- **Transparency** – eIDAS provides a list of trusted services that may be used within a centralised signing framework.

eIDAS defines standards for which advanced and qualified electronic signatures, qualified digital certificates, electronic seals, timestamps and other proof for authentication mechanisms to ensure that electronic transactions have the same legal standing as paper transactions.

eIDAS regulates advanced and qualified electronic signatures, electronic transactions, involved bodies and their embedding processes to provide a secure way for users to conduct business online like electronic funds transfer or transactions with public services. Both the signatory and recipient have access to a higher level of usability and security. Both sets of parties are able to perform transactions across borders.

For example, an advanced electronic signature is defined as one that meets all of:

- It is uniquely linked to the signatory

- It is capable of identifying the signatory

- It is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control

- It is linked to the data signed in such a way that any subsequent change in the data can be detected

2.5 European Union Agency for Network and Information Security (ENISA)

ENISA (https://www.enisa.europa.eu/) provides expertise on network security in Europe.

ENISA have documented (***Privacy and Data Protection by Design*** - https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-

design/at_download/fullReport) their view of what needs to be done to achieve privacy and data protection by default. For example, it specifies that encryption and decryption operations must be carried out locally and not remotely because both encryption/ decryption keys and data must remain in the power of the data controller and processor if any privacy is to be maintained. The report covers topics such as the use of cloud data storage where the data controller, not the cloud service provider, holds the encryption/ decryption keys.

ENISA have also documented (Handbook on Security of Personal Data Processing https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing/at_download/fullReport) guidelines for small to medium businesses on data security.

ENISA have documented the opportunities and issues relating to data protection certification (***Recommendations on European Data Protection Certification*** https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification/at_download/fullReport).

2.6 Article 29 Working Party

The Article 29 Working Party was established under Article 29 ***Working Party on the Protection of Individuals with Regard to the Processing of Personal Data*** of the Data Protection Directive http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046. Article 30 of the Directive describes the scope of its work.

Working Party was composed of representatives of the Supervisory Authority of each Member State, of representative from relevant or authorities established for the Community institutions and bodies and of a representative of the Commission. The Working Party had an advisory status and acted independently.

The Working Party produced much useful material on the implementation and operation of GDPR including:

Document	**Link**
Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation	http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826
Guidelines on Data Protection Impact Assessment (DPIA)	http://ec.europa.eu/newsroom/document.cfm?doc_id=47711
Guidelines on Data Protection Officers	http://ec.europa.eu/newsroom/document.cfm?doc_id=44100
Guidelines on Personal Data Breach Notification Under Regulation 2016/679	http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827
Guidelines on the Application and Setting of Administrative Fines	http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889
Guidelines on the Lead Supervisory Authority	http://ec.europa.eu/newsroom/document.cfm?doc_id=44102
Guidelines on the Right to "Data Portability"	http://ec.europa.eu/newsroom/document.cfm?doc_id=44099
Elements and Principles to be Found in Binding Corporate Rules (BCR)	http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798

All previous and archived content of the Article 29 Working Party is available from http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/index_en.htm.

2.7 European Data Protection Board (EDPB)

The Article 29 Working Party will transition to the EDPB. This has not yet been formed.

The main functions of the board will be:

- To issue guidance for controllers and processors on aspects of GDPR
- To support businesses ability to comply
- To determine disputes between national supervisory authorities
- To provide consistency across all member states and cooperate with Data Protection Authorities

2.8 European Data Protection Supervisor (EDPS)

This is an existing function established in January 2004 - https://edps.europa.eu/ . It is an independent data protection authority.

The objectives of this organisation are:

- To monitor and ensure the protection of personal data when EU institutions processes personal data
- To provide advice to EU institutions on subjects relating to the processing of personal data
- To provide advice to EU legislators on any proposals that may affect personal privacy
- To monitor technology developments and initiatives that may affect the protection of personal data
- To intervene before the Court of Justice of the EU to provide expert advice on interpreting data protection legislation
- To work with national supervisory authorities and other supervisory entities to ensure consistency in protecting personal data across the EU

3. Personal Information

Information is personal if it is:

- Owned by a person
- About a person
- Directed towards a person
- Sent or posted or communicated by a person
- Experienced by a person
- Relevant to a person

The definition of what is personal data is broad and includes all of the following:

Personal Data Type	**Personal Data Items**
Personal Information	Name, such as full name, maiden name, mother‘s maiden name, or alias
	Date of birth
	Place of birth
	Full home address
	Country, state, postcode or city of residence
	Marital status
	Telephone numbers, including mobile, business and personal numbers
	Information identifying personally owned property, such as vehicle registration number
	Passport number
	Social insurance or national insurance number
	Residence and geographic records
	Sexual orientation
Biographical Data	Specific age
	Height
	Weight
	Eye colour
	Hair colour
	Photographic image
	Gender
	Racial or ethnic origin
	Any defining physical characteristics
Digital footprint	Digital identities, such as avatars and usernames/handles
	Logon details such as name, screen name, nickname, or handle
	Email address (if private from an association/club membership, etc.)
	IP addresses (in the EU)
	Geo-tracking information and location-based data
	Web usage behaviour or user preferences using persistent cookies
	Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address
	(MAC) address or other host-specific persistent static identifier that consistently
	Any information that links a particular person to a small, well-defined group
Medical or Heath Data	Patient identifier
	Number of sick days taken from employer and other information relating to any sick leave

Personal Data Type	**Personal Data Items**
	Visits to doctors
	Medical data
	Biological traits including DNA
	Fitness data
	Medical images such as X-rays, CT scans and ultra sound
	Biometric data such as fingerprints, retinal scans, voice signature or facial geometry
	Medication

The definition of personal data is very important. It does not just include information a person explicitly supplies. It includes implicit information such as browsing history.

GDPR identifies special categories of personal data for which processing is subject to additional constraints. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

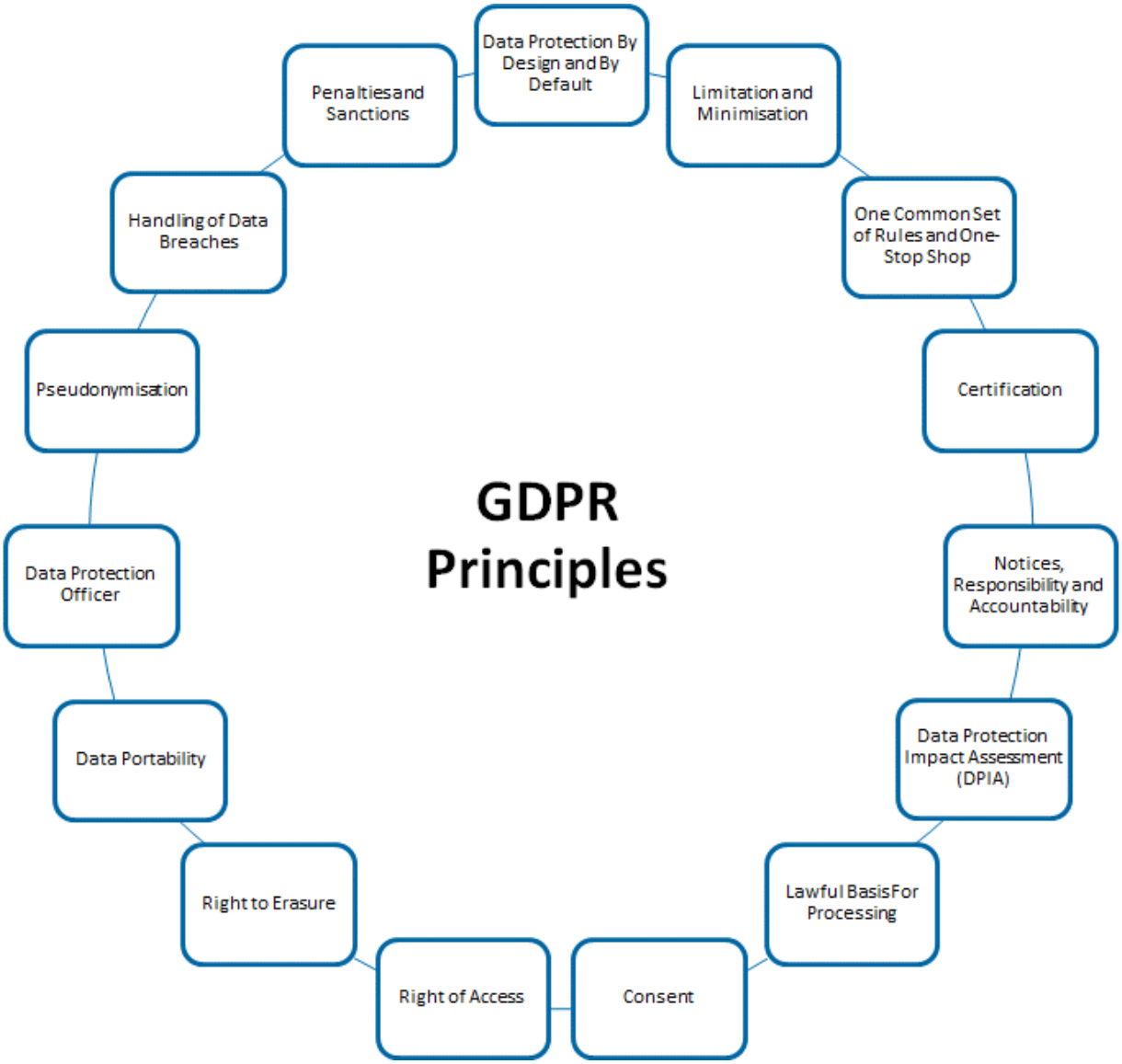
4. Principles of GDPR

4.1 Overview

GDPR extends the existing Data Protection framework. The data controller (an entity that collects data from EU residents) or processor (an entity that processes data, either directly or indirectly such as on behalf of data controller) or the data subject (individual) is based in the EU. The regulation also applies to entities based outside the EU if they collect or process personal data of EU residents.

There are core principles that underpin the operation of the GDPR. These include:

1. Data Protection By Design and By Default
2. Limitation and Minimisation
3. One Common Set of Rules and One-Stop Shop
4. Certification
5. Notices, Responsibility and Accountability
6. Data Protection Impact Assessment (DPIA)
7. Lawful Basis For Processing
8. Consent
9. Right of Access
10. Right to Erasure
11. Data Portability
12. Data Protection Officer
13. Pseudonymisation
14. Handling of Data Breaches
15. Penalties and Sanctions



The next sections summarises the key elements of these principles. This is not intended to be exhaustive.

4.2 Data Protection By Design and By Default

Article 25 of the GDPR requires that data protection is designed into the development of business processes for products and services. By default, privacy settings must be set at a high level.

The organisation must implement mechanisms to ensure that personal data is only processed when necessary for specific purposes and complies with the regulation throughout the data processing lifecycle.

Data Protection By Design and By Default requires a combination of systems and processes. Changes to existing IT systems and possible new IT systems will be required to achieve this.

Section 5.4 on page 36 contains more details on implementation options.

4.3 Limitation and Minimisation

The collection of personal data should limited for specific and justifiable purposes. The amount of personal data collected should be minimised. The storage interval should be limited. The type of processing should

be limited and necessary. There should be a legal basis for processing. Access should be controlled and excluded by default rather than being inclusive. Processing of special categories of personal data should be avoided unless absolutely required. Data security should occur as a matter of course.

Essentially, if there are any doubts and the data is not necessary do not collect it. Keep it simple.

4.4 One Common Set of Rules and One-Stop Shop

There will be one set of data protection rules across all EU member states.

Each state must create an independent Supervisory Authority (SA) to hear complaints, investigate them and to take administrative actions and enforce sanctions.

Where an entity such as a multi-national has multiple locations in multiple EU states, it will have a single SA as its lead Supervisory Authority, based on the location of its main office. In this instance, the lead SAS will act as a one-stop shop to supervise all the processing activities of that business throughout the EU.

4.5 Certification

GDPR call for a voluntary data protection certification regime to be established. Data protection seals and marks should be created to demonstrate GDPR compliance by of data processing operations by data controllers and data processors.

Where it exists, certification will last for a maximum period of three years. It may be renewed.

The register of such compliance should be publically available.

For more details on possible certification approaches documented by ENISA see section 2.5 on page 11.

4.6 Notices, Responsibility and Accountability

4.6.1 Notices

The need for and the content of privacy statements on web sites and other entry points to digital information and services that was specified in the Data Protection Directive has been expanded.

These privacy statements must now include the retention time for personal data and contact information for data controller and data protection office of the organisation.

The notice must be concise, transparent, intelligible and readily accessible. It must be written in clear and plain language. This is particularly true if your web site is aimed at children.

Article 13 of the GDPR specifies the information the privacy notice needs to contain.

There can be one general notices or several notices throughout the web site on those pages where personal information is being collected. It is best practice to include notices on all pages where personal information is required to be entered.

General Privacy Notice Contents	**Specific Personal Information Collection Privacy Notice Contents**

Identity and the contact details of the data controller	The length of time for which the personal data will be stored, or if that is not possible, the criteria used to determine it
Contact details of the data protection officer, if one exists – see below	The right to: • Request from the data controller access to • Request rectification or erasure of personal data • Restrict processing • Object to processing • Data portability
The purposes of the processing of personal data and the legal basis for this processing (Article 6 Lawfulness of Processing)	The right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
Who receives the personal data	The right to complain to Supervisory Authority
Whether data is being transferred to a third country or international organisation and, if so, the safeguards that are being used and the means by which to obtain a copy of them or where they have been made available	If the provision of personal data is a statutory or contractual requirement or necessary to enter into a contract, as well as whether the person is obliged to provide the personal data and of the possible consequences of failure to provide the data
	The use of automated decision-making, including profiling and where this applies meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the person

If the data controller intends to process the personal data for a purpose other than the ones for the personal data was originally collected, the data controller must provide the person with details on that other purpose before that processing takes place.

4.6.2 Responsibility and Accountability

The principle of Privacy By Design and By Default requires that data protection measures are designed and incorporated into the development of business processes and systems...

The data controller is responsible for implementing effective measures and being able to demonstrate the compliance of processing activities even if the processing is carried out by a separate data processor on behalf of the data controller.

Personal data must be pseudonymised as soon as possible after collection and expiry of its original use.

4.7 Data Protection Impact Assessment (DPIA)

Before there were DPIAs there were Privacy Impact Assessments (PIAs). So many organisations will already have experience of this type of assessment. Much of the approach used to conduct PIAs can be reused when performing DPIAs.

Performing a DPIA is not mandatory for every processing operation. A DPIA must be conducted when specific risks occur to the rights and freedoms of persons. The Supervisory Authority must supply prior approval for high risks. The data controller must perform risk assessment and mitigation for these high risks.

The rights and freedoms referred to primarily relate to the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.

Failure to carry out a DPIA when the processing requires one, carrying out a DPIA incorrectly or failing to consult the Supervisory Authority where required can result in an administrative fine.

The scope of the DPIA and the contents of its outputs includes:

- Details on why the DPIA is being performed
- Description of the purposes of the processing
- Detailed description of the steps involved in the data processing operations – this should include the flow of personal data through the systems and business processes as business activities are performed
- Assessment of why the processing is being performed and how this is proportional to the underlying need
- Identification of the risks to the rights and freedoms of the persons affected
- The actions being taken to address the risks identified such as system and process changes
- The implementation of the actions
- Demonstration how the process and the risk mitigation complies with GDPR
- Where a high risk has been identified, the organisation must submit the DPIA to Supervisory Authority for consultation
- Record of signoff of the DPIA by the responsible persons in the organisation

The GDPR identifies nine criteria should be considered to assess if the processing is likely to result in a high risk.

4.8 Lawful Basis For Processing

Personal information can only be processed if there is at least one lawful basis to do so. The lawful reasons for this processing data:

- The person has consented to the processing of their personal data for one or more specific and prior notified purposes
- It is needed for the performance of a contract to which the person is a party or in order to take steps at the request of the person before to entering into a contract
- It is required to protect the vital interests of the person in question or of another person.
- It is required so the data controlled can comply with a specific legal obligation
- It is needed to perform a task carried out in the public interest or in the exercise of an official function of data controller
- It is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the person is a child

4.9 Consent

Even if the processing is lawful explicit consent of the person must be obtained for data collection and processing. Where the person is a child, the consent must be given by the child's parent or custodian. This consent must be and verifiable. Data controllers must be able to prove consent by recording when and how it was obtained. The person must have the opportunity to withdraw consent at a later stage.

Silence or implied consent and pre-checked boxes on web pages are no longer valid. The organisation must ask for consent and obtain explicit consent.

Consent must be specific. Where the data processing has multiple purposes, consent should be given for all of them.

The burden of proof that consent was obtained in a correct and explicit manner resides with the data controller. Consent management needs to include both the recording of consent and the circumstances under which it was provided.

Consent should be informed. The identity of the controller and the processing purposes should be detailed. Plain language should be used.

4.10 Right of Access

Persons have the right to access their personal data and to get details about how this personal data is being processed.

On request, the data controller has to provide:

- An overview of the categories of data that are being processed
- A copy of the data itself
- How it acquired the data
- Details on the processing such as the its purposes
- With whom the data are shared

4.11 Right to Erasure

A person has the right to request erasure of and cessation of processing personal data including any copies related to them:

- Where the personal data are no longer necessary in relation to the purposes for which they are collected
- Where the person has withdrawn their consent
- Where the person objects to the processing and there are no overriding legitimate grounds for the processing
- Where the processing of the personal data does not otherwise comply with the GDPR

For legal rulings and case law on the processing of personal data, see

> Internet search engine operators are responsible for the processing that it carries out of personal information which appears on web pages published by third parties
>
> **Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González** http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

Referring to persons on a publically accessible web page and identifying them either by name or by other means constitutes processing of personal data by automatic means

Bodil Lindqvist v Åklagarkammaren i Jönköping
http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=en

A data protection authority cannot enforce the applicable data protection law and impose sanctions against a controller that is not established in its jurisdiction. This is moot because of GDPR. Persons will be able to complain to their national data protection authority (the one-stop shop) that will then work with the supervisory authority in the country where the company is headquartered to ensure the rights of persons are protected when personal data is being processed.

Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság
http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN

Transfer of personal data

Case C-362/14 (Schrems)
http://curia.europa.eu/juris/document/document.jsf?docid=169195&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=452958

4.12 Data Portability

A person must be able to transfer their personal data from one controller to another without being prevented by the data controller. This covers both the information content – what was supplied – and the metadata.

The data must be provided in a structured and commonly used electronic format.

Portability includes the right to have personal data transmitted directly from one controller to another "where technically feasible". The GDPR does not define "technically feasible".

Data controllers are encouraged to develop interoperable formats that enable data portability but without there is no obligation for data controllers to adopt or maintain processing systems which are technically compatible with one another. Data controllers are prohibited from establishing barriers to transmission.

Requests should be processed within one month of receipt of the request. This one month period can be extended to a maximum of three months for complex cases as long as the person has been informed about the reasons for such delay within one month of the original request.

4.13 Data Protection Officer (DPO)

It is mandatory for certain data controllers and data processors - all public authorities and organisations that, as a core activity, monitor individuals systematically (such as tracking and profiling on the Internet) and on a large scale or that process personal data on a large scale - to assign a person to the DPO role. Note that he GDPR does not define what constitutes a public authority. This will be determined by national law. Large scale is also not formally defined. Earlier drafts of the GDPR defined large-scale as the processing of data on more than 5,000 subjects in any 12-month period though this is not defined in the final version. So large-scale is not that large.

DPOs are not personally responsible for compliance with the GDPR. It is the data controller or data processor that is required to ensure and to be able to demonstrate that data processing is performed in accordance with GDPR.

DPOs must also be given sufficient autonomy and resources to carry out their tasks effectively. The DPO can be viewed as a mini-regulator.

The DPO should be skilled and experienced in managing IT processes, data security (including dealing with network attacks) and be knowledgeable in the issues around the holding and processing of personal and sensitive data. The skills required depend on the organisation and the processing it performs. The DPO should also know the administrative rules and procedures of the organisation. The organisation should include the DPO in all issues relating to the protection of personal data in a timely manner.

4.14 Pseudonymisation

Pseudonymisation means changing personal data so that the resulting data cannot be attributed to a specific person without the use of additional information. Encryption is a form of pseudonymisation. The original data cannot be read. The process cannot be reversed without the correct decryption key. GDPR requires that this additional information be kept separate from the pseudonymised data.

Pseudonymisation reduces risks associated with data loss or unauthorised data access

Note that pseudonymised data is still regarded as personal data and so remains covered by the GDPR.

It is viewed as part of the Data Protection By Design and By Default principle.

Pseudonymisation is not mandatory. Implementing pseudonymisation with existing IT systems and processes would be complex and expensive. Pseudonymisation is an example of unnecessary complexity within the GDPR.

4.15 Handling of Data Breaches

It is impossible to have 100% security 100% of the time and still collect and process information. So organisations should assume a data breach however minor will happen at some time. It is important to reduce the scope and effect of the breach, the time to identify that the breach has occurred and to respond more quickly and effectively to limit the damage.

Organisations are responsible for the implementation and operation of sufficient countermeasures to prevent as much as possible, detect and handle breaches. A data breach in itself will not necessary attract administrative sanctions. The failure to have structures in place to prevent, detect and handle breaches will.

Data controllers have a legal obligation to notify the Supervisory Authority of a personal data breach within 72 hours (and if not an explanation of the delay) after having become aware of the data breach. There is no de minimis standard for data breaches.

This notification must include:

- A description of the nature of the personal data breach including, if possible, the categories and approximate number of persons affected and the categories and approximate number of personal data records affected

- The name and contact details of the data protection officer or other contact point where more information can be obtained

- A description of the likely consequences of the personal data breach

- A description of the measures taken or that are proposed to be taken by the data controller to address the personal data breach, including any measures to mitigate its possible adverse effects

Persons affected by the data breach must be notified if the breach is likely to have a high risk to their rights.

Data controllers do not have to notify affected persons if protection measures were implemented that rendered the personal data unintelligible.

4.16 Penalties and Sanctions

Failure to comply with GDPR can result in penalties and sanctions. These include:

- Warnings
- Data protection compliance audits
- Fines

There are two levels of fines:

1. €10,000,000 or up to 2% of the annual worldwide turnover of the preceding financial year, whichever is the greater, for failures relating to:

    - Conditions applicable to child's consent in relation to information society services
    - Failures in data processing and security
    - Notification of a personal data breach to the supervisory authority
    - Communication of a personal data breach to the data subject
    - Data protection impact assessment
    - Designation of the data protection officer
    - Certification

2. €20,000,000 or up to 4% of the annual worldwide turnover of the preceding financial year, whichever is the greater for failures relating to:

    - Principles relating to processing of personal data
    - Lawfulness of processing
    - Conditions for consent
    - Processing of special categories of personal data
    - Information and access to personal data
    - Information to be provided where personal data are collected from the data subject
    - Right of access by the data subject
    - Right to rectification
    - Right to erasure
    - Right to restriction of processing
    - Right to data portability
    - Automated individual decision-making, including profiling
    - Transfers of personal data to third countries or international organisations

These fines are very large. It will be interesting to see how they are actually applied.

5. Implementing and Operating GDPR

5.1 Introduction

GDPR compliance is achieved through a combination of processes and technology.

Most of the impact that GDPR will have is on existing IT systems that process personal data.

The effort to implement and operate GDPR will depend on the scope of the problem which is dictated by the amount of personal data your organisation collect and processes.

Small, service-oriented companies generally collect little personal information and process it even less. So the compliance effort is quite small.

Larger companies that have large customer bases such as utility-type providers or providers of outsourced services such as cloud service providers or providers of web-based services and/or communications.

The problem with many compliance initiatives – recent financial-services oriented examples include EMIR, BCBS 239, Solvency II, MiFID II, Basel III/CRD IV, AMLD IV, PSD 2, FATCA and IFRS 9 – is that they tend to be treated as single projects operating in an organisation silo rather than as being part of a wider and more general and shared compliance framework.

Despite have a broad scope across the organisation, GDPR compliance will more likely in many cases be treated as yet another stand-alone initiative.

Organisations could expend a large amount of resources, expense and time implementing detailed GDPR compliance processes and systems that will only be used infrequently. Many organisations are taking minimalist or wait-and-see or watching brief type approaches to GDPR.

The types of systems needed to support the operation of GDPR will be similar to those implemented by public bodies to handle Freedom of Information requests. GDPR effectively applies Freedom of Information to all personal information maintained by organisations and extends its application to all organisations and not just public service bodies. When implementing the provisions of the various Freedom of Information laws, public service bodies generally implemented simple request tracking systems – see section 5.2.7 on page 31 – rather than making changes to the underlying systems that held the information. However, the provisions of GDPR are substantially more extensive than Freedom of Information covering data erasure and portability that will require changes to the core information storage and processing systems.

It is simply not possible to quantify the volume and types of requests that individuals will make under GDPR.

5.2 Preparatory Steps

At a high-level, the initial set of steps to be performed to start the process to achieve compliance is:

1. Determine your organisation's role under the GDPR – data controller or data processor
2. Assign someone to the Data Protection Officer role
3. Implement consent management
4. Review and update data retention and data backup
5. Identify and document business processes and associated IT systems processing personal data
6. Identify and assess any cross-border data flows

7. Prepare for persons exercising their GDPR rights
8. Prepare for a data breach

From these initial steps a GDPR compliance strategy and approach can be developed. This can include your organisation's approach to data governance and management, privacy management and security management.

If your organisation has subsidiaries perform these activities for each and then consolidate.

5.2.1 Determine Your Organisation's GDPR Role

Almost every organisation will be a data controller because they will collect some form of personal data about persons such as customers or employees.

If your organisation is outside the EU but offers goods or services to people in the EU or you collect behaviour-related information (such as web site access activity) of people residing in the EU or you process personal data on EU citizens on behalf of any organisation based in the EU then your organisation comes under the scope of the GDPR.

Inform your employees about GDPR risks and appropriate behaviours by defining clear policies on the collection and use of personal data and any collaboration and sharing or maintenance of local uncontrolled copies. Implement security awareness and privacy training.

5.2.2 Fill the Data Protection Officer Role

The primary role DPO is to ensure the organisation is compliant with GDPR. Many organisations are obliged to appoint a DPO such as:

- The organisation is a public body
- Processing operations require regular and systematic monitoring
- The organisation has large-scale processing activities, especially with special categories of personal data

Earlier drafts of the GDPR defined large-scale as the processing of data on more than 5,000 subjects in any 12-month period though this is not defined in the final version. So large-scale is not that large.

Initially, appoint someone to the DPO role irrespective of any legal necessity. The role does not have to be full-time. Once compliance is achieved the level of work may reduce.

The DPO role is cross-functional. It spans the entire organisation, crossing the boundaries of business functions. These roles are often very difficult to implement as they encroach on the territories of business function leaders and, in doing so, encounter resistance.

So the DPO role needs to be supported from the highest levels in the organisation. Otherwise it will not be successful.

5.2.3 Implement Consent Management

Consent management involves:

- Identify all points where personal data is collected across all communication channels

- Identify the data processing processes where consent is required
- Draft GDPR consent management notices
- Update communication channels such as the organisation web site(s) with GDPR consent notices
- If data is collected from children, implement an approach to collect consent from parents or guardians
- Update IT systems to record consent details and allow consents be subsequently updated

5.2.4 Review and Update Data Retention and Backup

At a high-level, the activities involved in this include:

- Reviewing existing approaches to data archival, retention and deletion, if any
- Reviewing data backup processes to ensure data not being retained is not held on backups
- Implement data retention and deletion policies and procedures
- Update data backup policies and procedures

5.2.5 Identify and Document Business Processes and Associated IT Systems Processing Personal Data

Create an inventory of personal data collected, created, processed and derived. Review the reasons why personal data is collected and stop collecting if it is not necessary or justifiable.

Identify any high-risk data collected or generated. Consider conducting DPIAs for these.

Identify if you process any of the special categories of personal data and handle this instances in more detail. Consider conducting retrospective DPIAs for these.

Where personal data is collected ensure explicit consent is obtained,

Develop and implement notices on all personal data collection points. Identify points where consent is necessary.

Create an inventory of business processes where personal data is involved. Appoint business process owners. Document these business processes with those involved in their operation. Define business process review dates, at least annually.

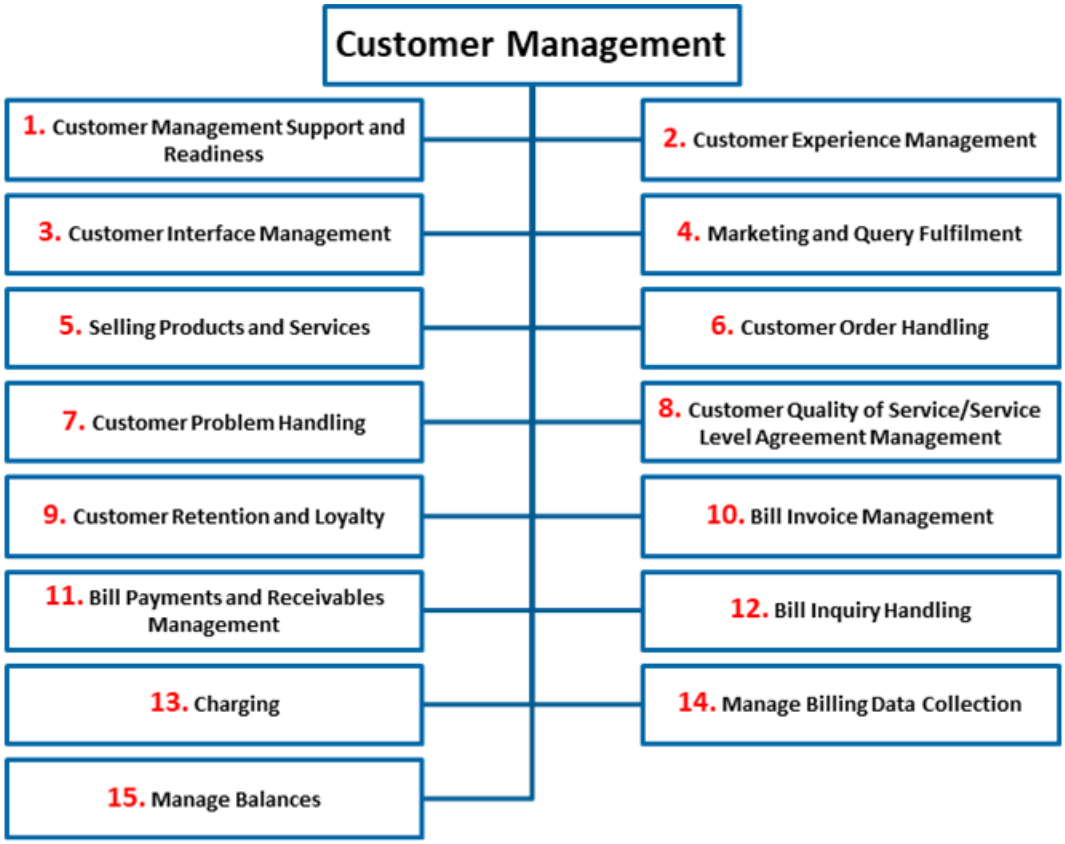
Document the legal grounds for processing this personal data.

Create an inventory of IT systems that store and process personal data.

Map the flow of personal data across business processes and IT systems from initial collection to its processing and ultimate deletion.

Consider initiating a business process review and update exercise that minimises the amount of personal data being collected and processes to reduce your compliance overhead and risk.

For example, the following shows a generic high-level breakdown of the sets of processes associated with managing customers. Each of these process areas will contain the actual business processes that collect and process personal data. A structured process representation and breakdown such as this is useful in organising a structured approach to process identification and description.



You can use a structure such as this to assist the creation of a business process inventory.

These generic processes relate to the acquisition and retention of customers.

They include retention management, cross-selling, up-selling and direct marketing.

All this involves collecting personal data directly or indirectly (behaviour related) and its processing to personalise and customise the service to customers as well as to identify opportunities for increasing the what is sold to the customer.

Much of this processing will now require explicit customer consent.

This data discovery and profiling work has the potential to be quite onerous, depending on the number of IT systems and processes involved in processing personal data.

Review your network security, especially on systems that contain personal data that can be accessed from outside the organisation

Identify any third-parties involved in data collection and data processing for your organisation such as IT outsourcing or business process outsourcing arrangements. The specific topic of GDPR and outsourcing is considered later in section6 on page 41. For each of these outside organisations you must ensure that they too are compliant with GDPR:

- Review their network security
- Review their data retention policies to ensure personal data is deleted as soon as it is no longer needed
- Review data backup processes and amend to ensure data not being retained is not held on backups
- Ensure they appoint a DPO
- Review their process for handling data breaches

Where suppliers fail to meet GDPR compliance requirements they must resolve these issues or you must replace them.

5.2.6 Identify and Assess Any Cross-Border Data Flows

The EDPS (see section 2.8 on page 13) has produced guidance on international data transfers – see https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en .

While this relates to the processing of personal data by Community institutions and bodies it can be used as the basis for a more general view on cross-border data flows.

Transfers to any of the 28 EU member states (the status of the UK after BREXIT is not currently defined) are still allowed as well as to Norway, Liechtenstein and Iceland, that is countries that are members of the European Economic Area (EEA).

The European Commission has Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay to have an adequate level of protection so data transfers to these countries are also possible.

In February 2016, after the previous Safe Harbour scheme was rendered invalid, the European Commission and the United States agreed on a framework for transatlantic data transfers called the EU-U.S. Privacy Shield. The European Commission officially deemed this to be adequate in July 2016 – see http://europa.eu/rapid/press-release_IP-16-2461_en.htm.

In the absence of adequacy decisions for particular countries you should use proper and suitable safeguards such as Binding Corporate Rules (BCRs) and contracts. BCRs are described in Article 47 of GDPR and in the working document created by the Article 29 Working Party (see section 2.6 on page 12) ***Elements and Principles to be Found in Binding Corporate Rules (BCR)*** http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798.

Any BCRs must be legally binding and must specify clearly the duties and responsibilities of each participating member of the group of undertakings or group of enterprises engaged in a joint economic activity including their employees. BCRs must apply to every member of the group.

The group of undertakings can include international organisations, business alliances, joint ventures, outsourcing arrangement, or shared economic activities.

The BCRs must explicitly specify:

- A duty and responsibility for an EU-based member of the group with delegated responsibilities to accept responsibility for and to agree to take the necessary action to remedy the acts of other members outside of the EU bound by the BCRs and to pay compensation for any material or non-material damages resulting from the violation of the BCRs by BCR members.

- If a BCR group member located outside the EU violates the BCRs, the courts or other competent authorities in the EU will have jurisdiction and the person will have the rights and remedies against the

BCR member that has accepted responsibility and liability as if the violation had been caused by them in the Member State in which they are based instead of the BCR member outside the EU.

The BCR should cover:

- Structure and members of the group sharing the joint economic activity
- Contact details of overall group and of each member
- Contact details for DPO function of each member
- Details on data protection training for staff with access to personal data
- Obligations towards the relevant supervisory authorities
- The tasks of any DPO or other business function responsible with compliance monitoring.
- Numbers or and details on the data transfers including the data being transferred
- Purpose of the data transfers
- Processing perform by each member of the group
- Legally binding obligations of each member towards one another and towards the persons whose data is being processed
- Statement of liability of data controller or data processor in EU with regards to breaches of the BCRs by any member outside the EU
- Persons rights, the ways to exercise those right including the right to complain
- Provision of information on the BCRs towards persons to meet obligations, duties and rights of information of the GDPR
- Complaint procedures and complaint handling
- Data protection audits including scope and frequency and the methods of correction to protect persons' rights
- Application of general data processing principles and generally accepted privacy principles

The topic of outsourcing is discussed further in section 6 on page 41. Bear in mind that cloud computing services are just another form of outsourcing.

This activity should also include:

- Review all external data processing arrangements, including data storage and use of external applications, that store personal data

- Determine the GDPR compliance of these processing arrangements and consider rationalising suppliers

- Review the contracts and agreements associated with these arrangements

- Update the agreements to include GDPR-specific details

- Review and update supplier selection and procurement processes to include GDPR-specific requirements in selection factors and in new service contracts

5.2.7 Prepare for Persons Exercising Their GDPR Rights

The operation of GDPR will give rise to the need to develop, implement and operate a number of business processes and associated standard operating procedures to implement the rights of persons under GDPR. The inventory of these processes includes:

- **Request Tracking** – All requests made under GDPR by persons and the request type must be recorded. The request type workflow needs to be initiated and the individuals and business functions within the

organisation allocated to work on the request should be tracked. The dates and times of the actions performed from the initial request should be logged. Reporting on the number of active requests, their status and any deadlines that apply should be recorded. Any correspondence and communications performed as requests are processed should be recorded.

- **Consent and Consent Recoding and Tracking** – Consent should be explicitly sought and recorded to establish an audit trail should the need arise to prove it at some future time.

- **Consent Withdrawal** – Persons should have the right to withdraw their previously granted consents. This means they should be able to see what consents they previously granted. The withdrawal of consent should be recorded to establish an audit trail should the need arise to prove it at some future time. Related systems should be updated to ensure that processing of the person's data is stopped.

- **Access to Data** – Persons have the right to request access to all personal data the organisation stores about them. This implies that there must be a record of all personal data including derived data held across all systems, including manually-maintained and paper records. The data from all these sources must be consolidated and supplied to the requestor.

- **Data Rectification** - Persons have the right to have inaccurate personal data rectified inaccurate personal data

- **Restriction of Processing** - Persons have the right to restriction of processing of their personal data where its accuracy is contested, the processing is unlawful and the person opposes the erasure of the personal data and requests the restriction instead, the data controller no longer needs the personal data for the purposes of the processing or the person has objected to processing and pending the verification of the objection

- **Data Objection** - Persons have the right to object that personal data processing is necessary for the performance of a task. The data controller can no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the person.

- **Profiling Objection** - Persons have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

- **Data Erasure** – persons have the right to have their data erased. This implies that there must be a record of all personal data including derived data held across all systems, including manually-maintained and paper records. The inventory of personal data must be consulted and the associated personal data for the requesting person deleted. The act of erasing personal data should be recorded.

- **Data Portability** – Portability is discussed in section 4.12 on page 22. Persons have the right to have their data transferred to another data controller. As with Access to Data and Data Erasure, this requires that there must be a record of all personal data including derived data and that this can be extracted into a format that can be transferred securely

- **Complaint Handling** – Persons can complain to their Supervisory Authority that may then forward the complaint to the organisation where it must be handled and responded to.

- **Personal Data Breach Notification** – Organisations must notify their Supervisory Authority of any data breaches.

- **Person Data Breach Notification** – When the data breach is likely to have a high risk to the rights of persons organisations must notify them of the breach.

- **Record of Audits of Third-Party Data Processors** – Organisations should regularly audit any third-parties they use for data processing and record the results of the audit.

This is lengthy list of processes. Their definition, implementation and operation have the potential to be onerous.

At a minimum the facility that tracks the receipt of requests, their processing, fulfilment and transmission of the response to the requestor should contain the following:

Field	**Description**
Date and Time Request Received	The date and time that the request is received from the individual/authorised entity
Received By	The person of business function who logged the request
Source	The source of the request
Request Type	The type of the request
Priority	A priority assigned to the request
Request Details	A description of the request
Requester Contacted for Clarification	A flag indicating if the requester needs to be or was contacted to clarification
Clarification Received	Notes on clarification received
Request Reviewed and Approved for Processing	A flag indicating that the request contains sufficient details to allow it to be processed
Date Request Processing Started	The date that formal response processing started. The due date is calculated from this date, based on the request type
Date Request Response Due	The due date of the response
Business Functions Affected by Request	A list of business functions within the organisation affected by the request
Third Parties Affected by Request	A list of third-parties within the organisation affected by the request
Request Sent to Business Functions <N>	Details on the request sent to the business function, date and time, person, details of request, date due, date received, clarification required and received. This will be repeated for each affected business function. There will be a sub workflow for each business function
Request Sent to Third Party <N>	Details on the request sent to the third party, date and time, person, details of request, date due, date received, clarification required and received. This will be repeated for each affected third party. There will be a sub workflow for each business function
Response Reviewed Date and Time	The date and time that the response is received and collated
Response Reviewed By	The person who reviewed the response
Response Redaction Required	A flag indicating that the response needs to be redacted before it is issued to the requester
Response Redaction Notes	Notes on the nature of and reason for the redaction of the response
Response Redaction Completed By	The person who completed the redaction
Response Redaction Reviewed By	The person who reviewed the redaction
Response Redaction Reviewed Date and Time	The date and time the redaction was reviewed and approved
Response Release Authorised By	The person who authorise the release of the response
Date and Time Response Issued	The date and time the response was issued
Response	The response or details on where the response is stored

Response Covering Communication	The covering communication that accompanied the response

5.2.8 Prepare for a Data Breach

At a high-level, the activities involved in this include:

- Identify Supervisory Authority contact details
- If you organisation is based outside the EU, identify an EU-based representative to handle breach notification and handling
- Document a list of breach scenarios and identify steps to be performed
- Create draft breach notifications including Supervisory Authority and personal contacts
- Document breach management process including roles and responsibilities

5.3 Approaches to Achieving Compliance

The owner of the business processes where personal data is collected and processed is responsible for compliance. The DPO is not responsible for compliance. The data protection officer assists with compliance. So the organisation should formally appoint business process owners. These business process owners should conduct privacy impact and risk assessments regularly.

Risk management plays a large part of achieving compliance with GDPR. Business process owners should be able to informed decisions on how to address risks in their data processing processes within the processes for which they are responsible. Risks can be mitigated until the residual risk is within tolerable limits.

Achieving compliance with GDPR should, in the first instance, focus on personal simplification, reduction and minimising the amount of personal data you collect and process, is possible.

Consider moving to excluding access to personal data by default.

Review any processing performed by third-parties, any outsourcing arrangements or use of cloud systems or platforms such as Dropbox, Google G Suite, Microsoft Office 365 or other similar systems.

Review your sourcing and supplier selection factors and ensure they explicitly include security controls, privacy management and privacy control functions, certifications and approach to auditing.

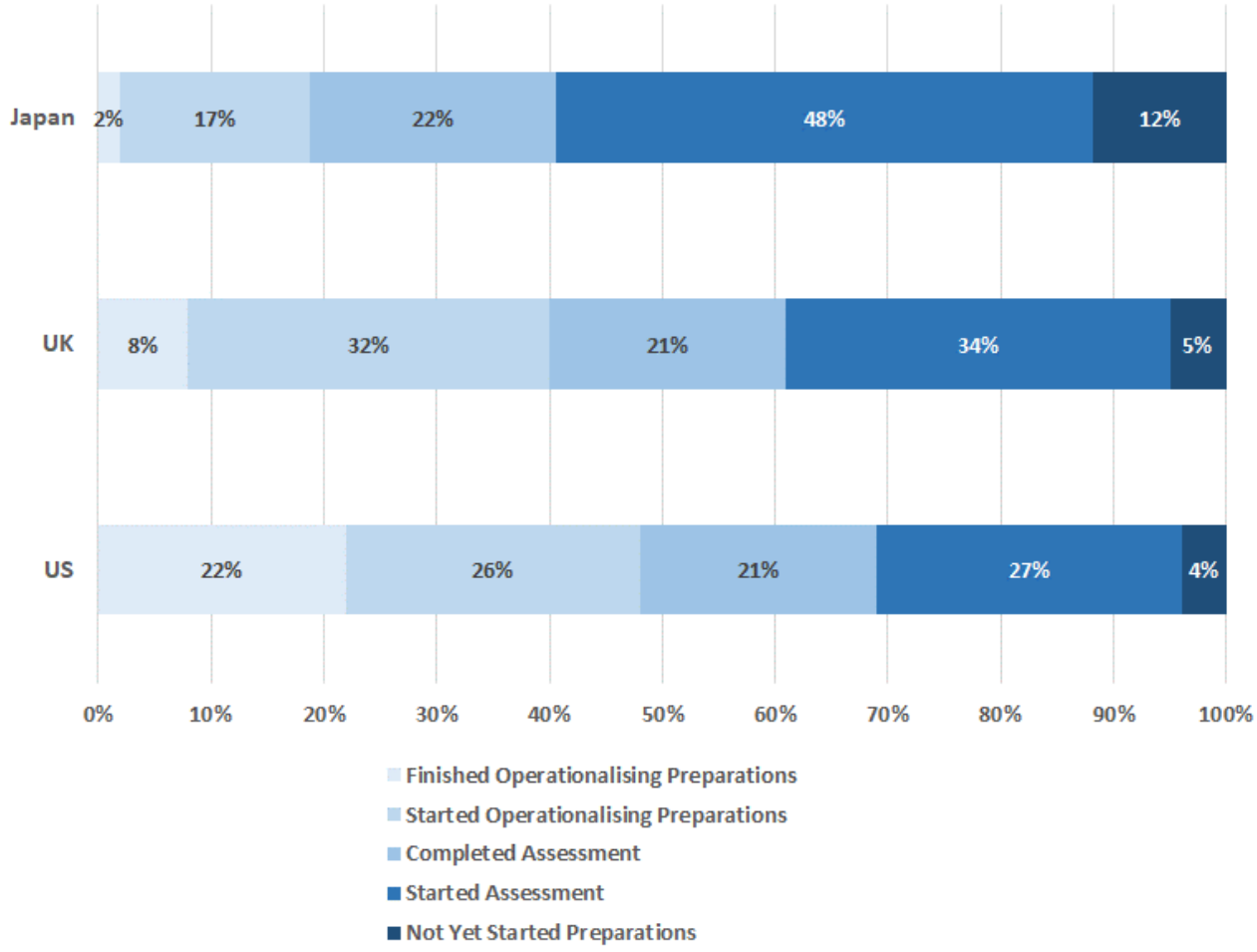
Note that mobile devices come under the ambit of GDPR if they are used for the processing of personal data. Data breaches occur when mobile devices are lost, resulting in unintended loss of control over personal data. A mobile device management facility including the ability to remotely wipe lost devices might be required. Previous Bring Your Own Device (BYOD) policies might need to be revisited employees do not consent to his personal device being remotely monitored and controlled.

Implementing and operating GDPR will have a cost. This will vary considerably depending on the size of the organisation

PwC have conducted a number of surveys on the GDPR preparations and estimated budgets for 300 large organisations in the UK, US and Japan. The most recent survey is from July 2017 –see

https://www.pwc.com/us/en/increasing-it-effectiveness/publications/general-data-protection-regulation-gdpr-budgets.html.

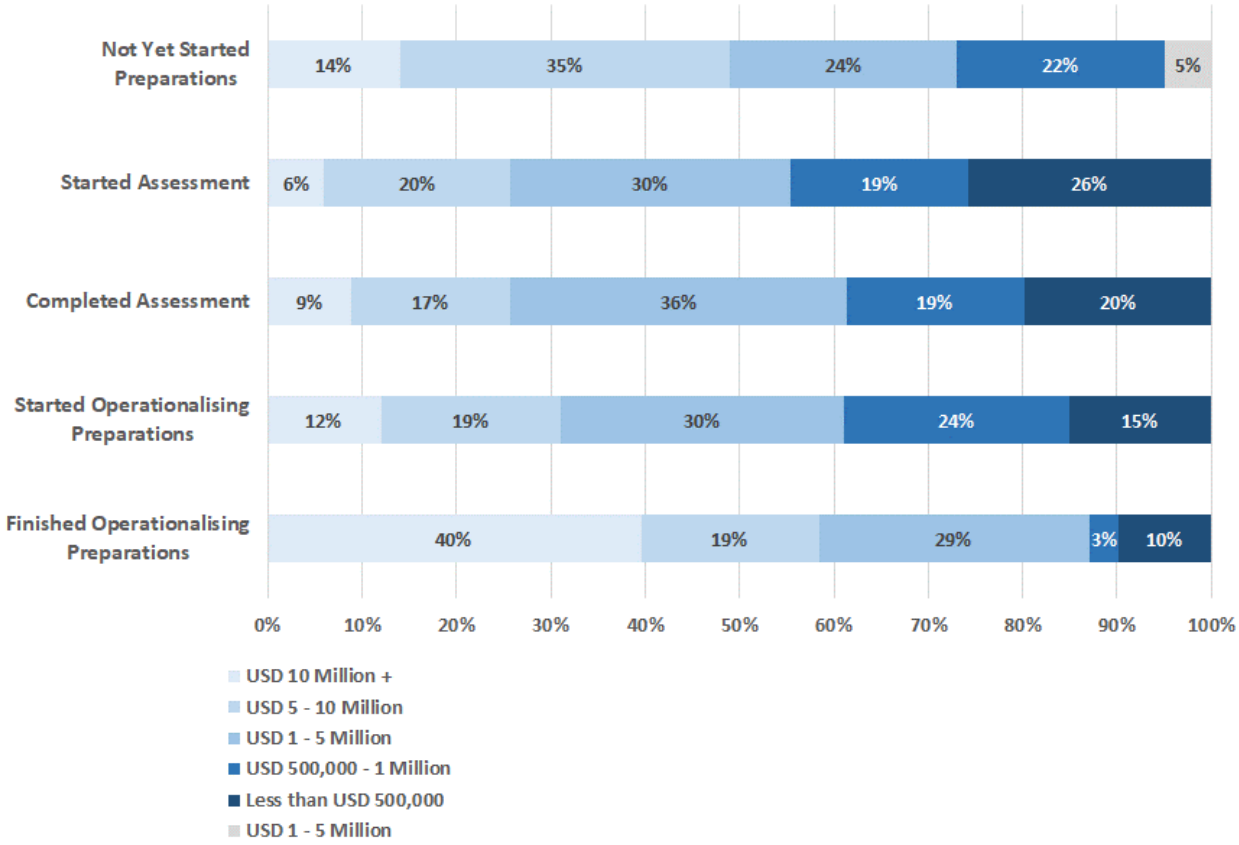
The status of preparations of these organisations is:



In July 2017, only 11% of executives surveyed said their companies have now finished operationalised preparations.

Of the companies who said they have finished preparations, 88% reported spending more than USD 1 million on GDPR preparations and 40% reported spending more than USD 10 million.

Among all companies, 60% said they plan to spend at least USD 1 million on GDPR preparation projects and 12% plan to spend more than USD 10 million.

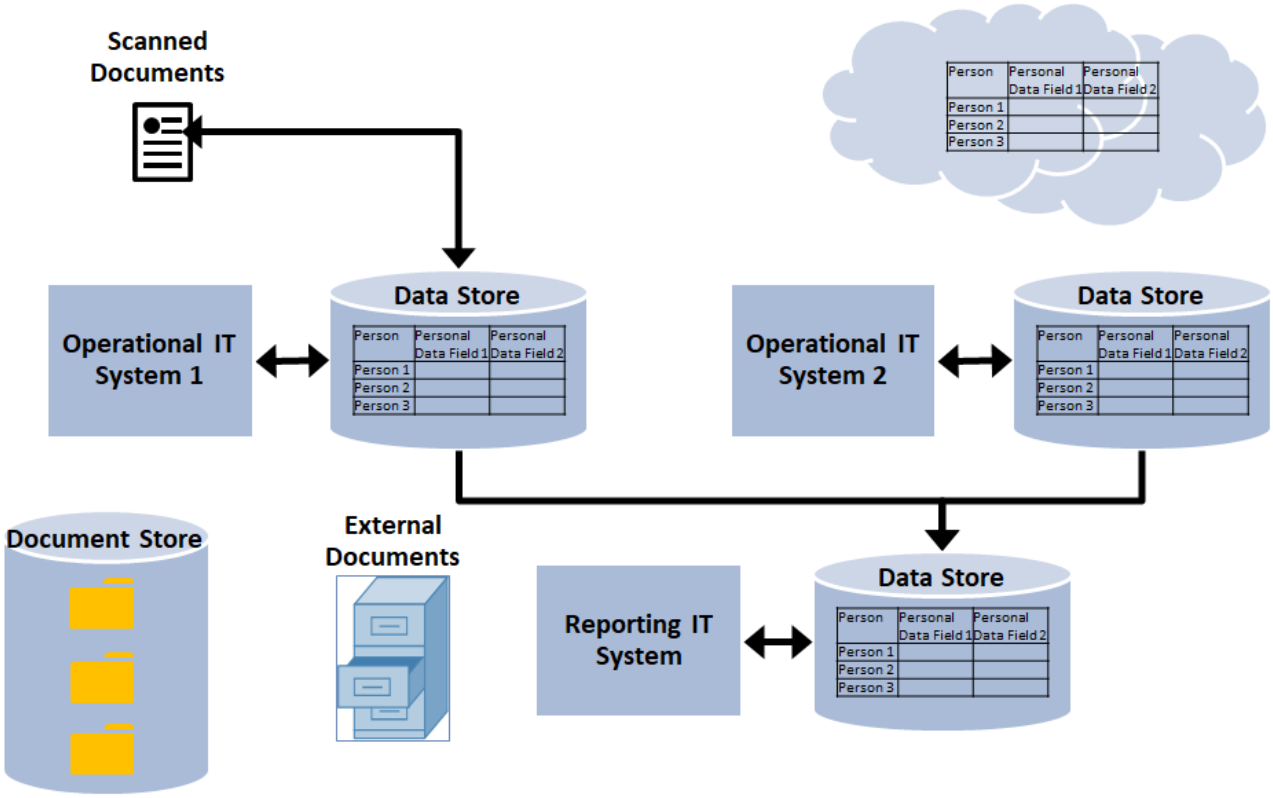


5.4 IT Systems and GDPR Compliance

Organisations will have multiple IT systems, each of which will store personal data. Personal data may also exist in the form of documents scanned into document management systems or documents generated and store in electronic folders or in email systems.

The same person will have different sets of data stored across these systems. The person may not uniquely identifiable across these systems. There may be variations in the spelling of names and addresses and different data formats.

Simplistically, the personal data landscape of an organisation can be represented as:



There will be separate internal operational IT systems.

There may be reporting systems that take data from operational systems.

Personal data may be stored on external systems, either for pure storage or for use by applications (such as marketing).

Documents generated using tools such as Microsoft Office will be stored both locally on individual users' PCs and on central file storage.

Personal information will also be contained on paper documents

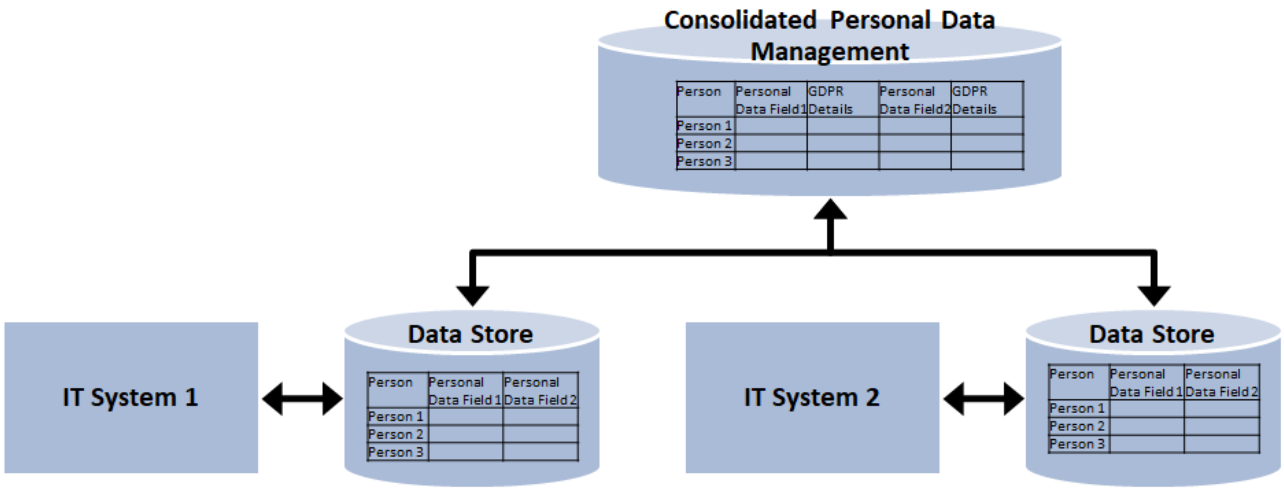
In the case of IT systems, there are broadly two options:

1. Modify each operational IT system to hold additional information such as GDPR flag indicating that the data is personal and comes under the scope of GDPR, retention details, consent details, deletion details

2. Implement a separate system that takes data from the operational systems and that create a single consolidated view of personal data across these systems

Option 1 is potentially very expensive and time consuming. If the IT systems are sourced from third-parties these organisations may over time update their systems to allow the additional GDPR-related information to be stored.

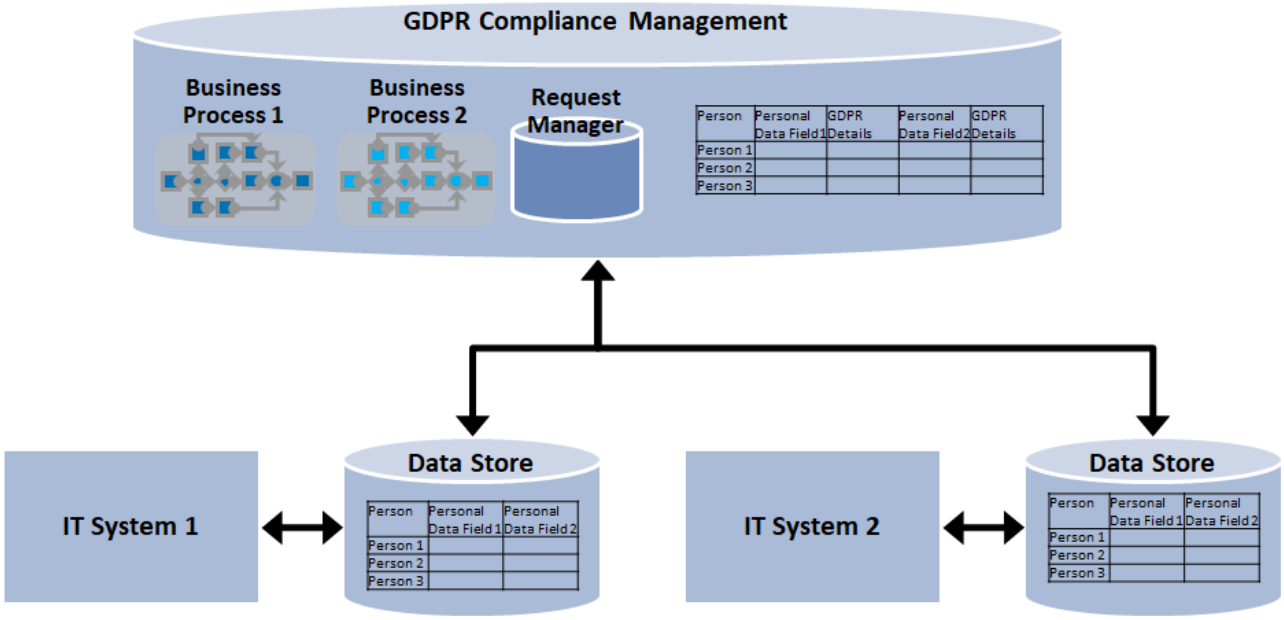
Option 2 involves developing or sourcing a software system to provide this consolidated personal data management functionality. One of the issues with having a separate system is that changes that occur in the underlying operational systems have to be reflected in it.



Note that both of these solution approaches just provide containers for GDPR-related information on personal data to be stored. That information has to be defined and completed and subsequently maintained.

The separate system approach can be extended to provide additional facilities for some or all of:

- Define and manage business processes that use personal data
- Log requests of various types and their processing
- Continuously monitor operational systems to identify changes in personal data
- Log details on personal data audits and DPIAs
- Data breach management
- Personal data access portal

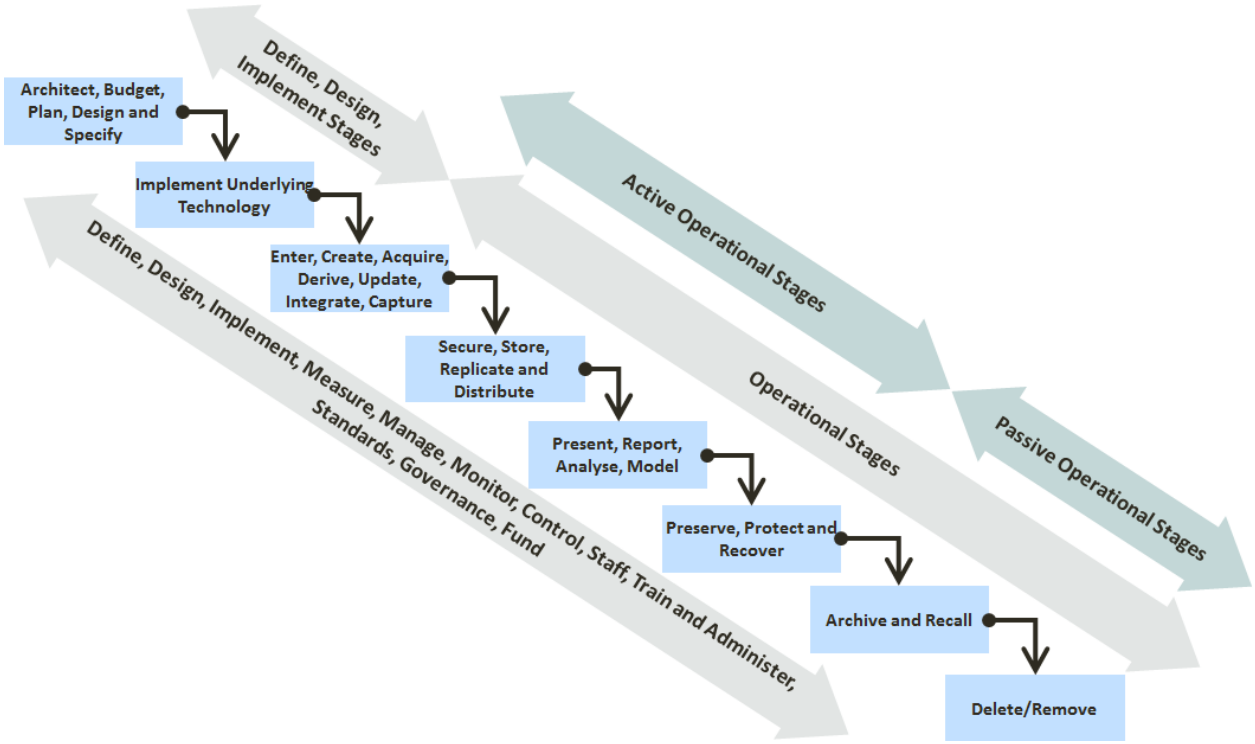


There are software vendors that offer such compliance solutions that provide some or all of the range of functions. However, the market is still embryonic and the optimum approach to achieving GDPR compliance is still uncertain. Investing in such technologies now may be premature.

There are vendors and developers of existing software products classified as Master Data Management (MDM) or Data Integration Hubs that offer similar facilities that may also be used.

5.5 Information Lifecycle View

Data has a lifecycle in the organisation, from its initial collection to its final archival and deletion. This can be represented in general terms in the following diagram:



The stages in this generalised information lifecycle are:

- **Architect, Budget, Plan, Design and Specify** - This relates to the design and specification of the data storage and management and their supporting processes. This establishes the data management framework

- **Implement Underlying Technology** - This is concerned with implementing the data-related hardware and software technology components. This relates to database components, data storage hardware, backup and recovery software, monitoring and control software and other items

- **Enter, Create, Acquire, Derive, Update, Integrate, Capture** - This stage is where data originated, such as data entry or data capture and acquired from other systems or sources

- **Secure, Store, Replicate and Distribute** - In this stage, data is stored with appropriate security and access controls including data access and update audit. It may be replicated to other applications and distributed

- **Present, Report, Analyse, Model** - This stage is concerned with the presentation of information, the generation of reports and analysis and the created of derived information

- **Preserve, Protect and Recover** - This stage relates to the management of data in terms of backup, recovery and retention/preservation

- **Archive and Recall** - This stage is where information that is no longer active but still required in archived to secondary data storage platforms and from which the information can be recovered if required

- **Delete/Remove** - The stage is concerned with the deletion of data that cannot or does not need to be retained any longer

- **Define, Design, Implement, Measure, Manage, Monitor, Control, Staff, Train and Administer, Standards, Governance, Fund** - This is not a single stage but a set of processes and procedures that cross all stages and is concerned with ensuring that the processes associated with each of the lifestyle stages are operated correctly and that data assurance, quality and governance procedures exist and are operated

To achieve compliance with GDPR, the lifecycles of personal data processes should be documented and formalised. In particular data archival, data retention and data deletion – stages in the information lifecycle that are currently infrequently not handled well, if at all – need to be implemented.

	Business Process 1	Business Process 2	Business Process 3	Business Process 4
Architect, Budget, Plan, Design and Specify				
Implement Underlying Technology				
Enter, Create, Acquire, Derive, Update, Integrate, Capture				
Secure, Store, Replicate and Distribute				
Present, Report, Analyse, Model				
Preserve, Protect and Recover				
Archive and Recall				
Delete/Remove				
Define, Design, Implement, Measure, Manage, Monitor, Control, Staff, Train and Administer, Standards, Governance, Fund				

6. GDPR and Outsourcing

Outsourcing of personal data processing occurs in many ways and is quite pervasive. It includes any third-party IT system or service provider that is located outside the organisation that is used to store and process personal data. It includes:

- Processes personal data on behalf of the organisation (BPO - Business Process Outsourcing)
- Provides information technology services (ITO – Information Technology Outsourcing)
- Specific outsourcing arrangements such as HRO – Human Resources Outsourcing, LPO - Legal Process Outsourcing, Outsourced Document Processing, Contact Centre Outsourcing
- Social media used to communicate with persons
- Marketing and contact systems
- External document storage
- External applications

The ultimate responsibility to comply with the GDPR ultimately lies with the organisation relying on these third parties. See section 5.2.6 on page 30 for more details on Binding Corporate Rules (BCRs).

There are existing standards and approaches that can be adopted for use with GDPR compliance. There is no need to develop new GDPR-specific standards and approaches. These existing, detailed, well-defined and well-proven frameworks and approaches can and should be used.

Service Organisation Controls (SOC) originally related to auditing of financial transactions performed by third-parties and the controls in place. Over time, these have been extended to cover the operation of the service and its compliance with security, availability, reliability, confidentiality and privacy. This evolution consisted of:

1993 – Statement on Auditing Standards (SAS) No. 70, Service Organisations
2008 – Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy
2010 – Standards for Attestation Engagements (SSAE) 16, Reporting on Controls at a Service Organisation
2011 – International Auditing and Assurance Standards Board (IAASB) issued International Standard on Assurance Engagements (ISAE) 3402, Assurance Reports on Controls at a Service Organisation
2015 – Updated Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy
2016 – Standards for Attestation Engagements (SSAE) 18, Reporting on Controls at a Service Organisation

These standards have been developed by American Institute of Certified Public Accountants (AICPA - https://www.aicpa.org/) and International Auditing and Assurance Standards Board (IAASB - https://www.iaasb.org/). While they originated from an auditing background, they are more widely and generally applicable.

The material can be reused and applied when drafting service agreements with third-party suppliers and in defining the controls to be applied and audited.

There are five core Trust Services Principles:

1. **Security** -The system is protected against unauthorised access, use, or modification
2. **Availability** - The system is available for operation and use as committed or agreed
3. **Processing Integrity** - System processing is complete, valid, accurate, timely, and authorised

4. **Confidentiality** - Information designated as confidential is protected as committed or agreed
5. **Privacy** – This applies the generally accepted privacy principles (GAPP)

The privacy principle addresses the system's collection, use, retention, disclosure, and disposal of personal information in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP). This closely mirrors the privacy principles of GDPR.

GAPP consists of 10 sub-principles:

1. **Management** - The entity defines documents, communicates, and assigns accountability for its privacy policies and procedures.

2. **Notice** - The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

3. **Choice and Consent** - The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

4. **Collection** - The entity collects personal information only for the purposes identified in the notice.

5. **Use and Retention** - The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.

6. **Access** - The entity provides individuals with access to their personal information for re-view and update.

7. **Disclosure to Third Parties** - The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

8. **Security for Privacy** - The entity protects personal information against unauthorized access (both physical and logical).

9. **Quality** - The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

10. **Monitoring and Enforcement** - The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

The IAASB principles and essential procedures for performing assurance engagements can be found in section INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS 3000 of:

http://www.ifrs.org.ua/wp-content/uploads/2014/11/2014-IAASB-HANDBOOK-VOLUME-2.pdf

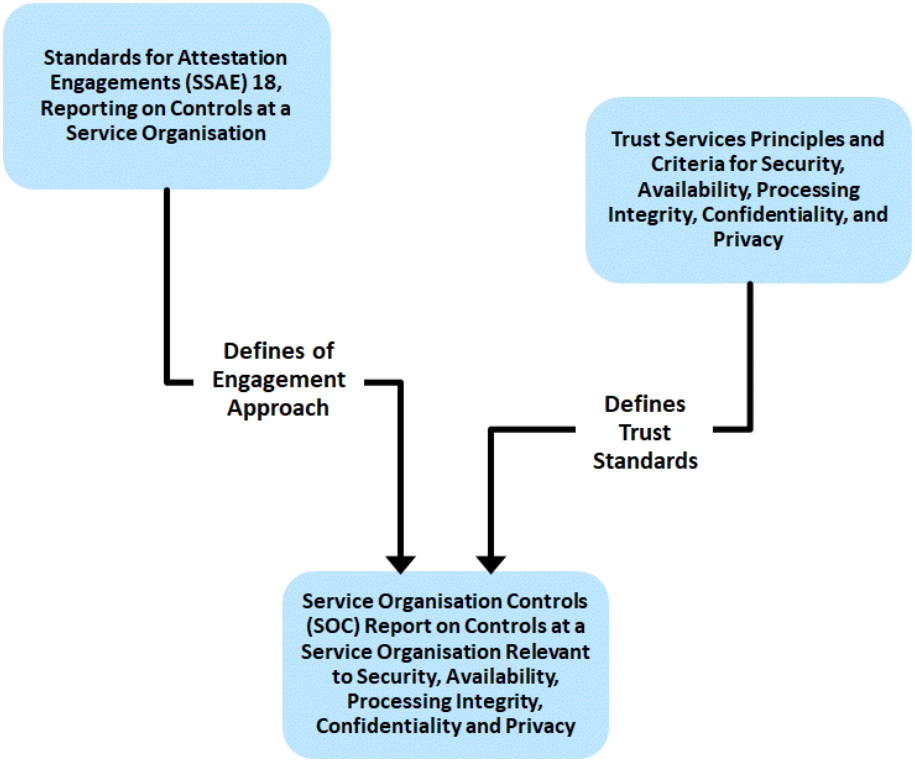
The detailed Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy document can be found at:

https://www.itm21st.com/Content/Documents/trustservicesprinciples-tsp100.pdf

The Service Organisation Controls (SOC) report is a formal review of the operation of these principles. More details on the SOC report covering Report on Controls at a Service Organisation Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy can be found at:

https://www.isaca.org/Groups/Professional-English/isae-3402/Documents/SOC2.pdf

The relationship between these standards is:



7. Data Governance

Data Governance is the exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets.

The scope of Data Governance is:

- To define, approve, and communicate data strategies, policies, standards, architecture, procedures, and metrics
- To track and enforce regulatory compliance and conformance to data policies, standards, architecture, and procedures
- To sponsor, track, and oversee the delivery of data management projects and services
- To manage and resolve data related issues
- To understand and promote the value of data assets

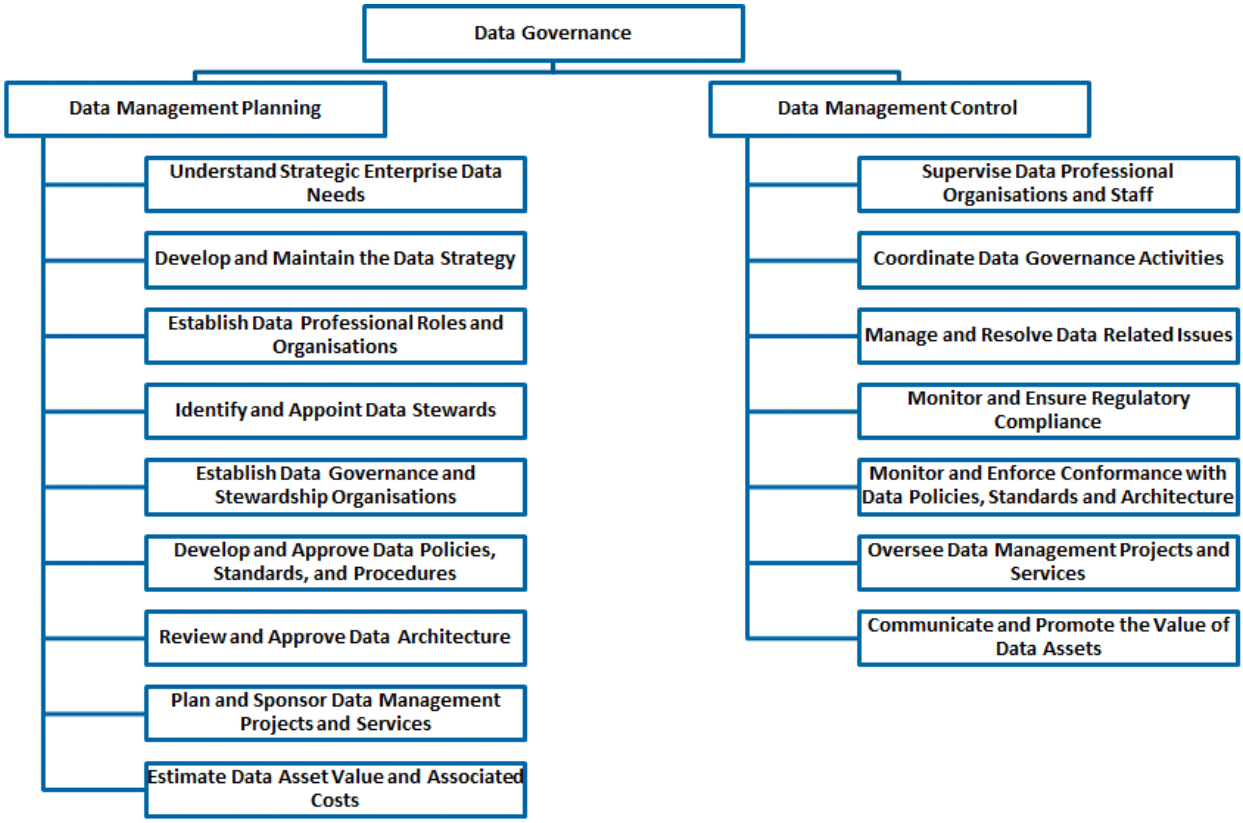
The objectives of Data Governance are:

- Guide information management decision-making
- Ensure information is consistently defined and well understood
- Increase the use and trust of data as an organisation asset
- Improve consistency of projects across the organisation
- Ensure regulatory compliance
- Eliminate data risks

Rather than being a siloed compliance project, GDPR belongs as part of a wider organisation data governance and even wider IT governance initiative.

Data governance is accomplished most effectively as an on-going program and a continual improvement process.

The approach to Data Governance includes:



This is:

- Data Management Planning
  - Understand Strategic Enterprise Data Needs
  - Develop and Maintain the Data Strategy
  - Establish Data Professional Roles and Organisations
  - Identify and Appoint Data Stewards
  - Establish Data Governance and Stewardship Organisations
  - Develop and Approve Data Policies, Standards, and Procedures
  - Review and Approve Data Architecture
  - Plan and Sponsor Data Management Projects and Services
  - Estimate Data Asset Value and Associated Costs

- Data Management Control
  - Supervise Data Professional Organisations and Staff
  - Coordinate Data Governance Activities
  - Manage and Resolve Data Related Issues
  - Monitor and Ensure Regulatory Compliance
  - Monitor and Enforce Conformance with Data Policies, Standards and Architecture
  - Oversee Data Management Projects and Services
  - Communicate and Promote the Value of Data Assets

Organisations need a realistic, practical and achievable starting point in order to implement good IT and data governance practices. When implementing initiatives that have a significant governance dimension, it is always easier, faster and cheaper to use an existing approach.

There are well-proven existing IT governance frameworks such as COBIT (Control Objectives for Information and Related Technologies) – see http://www.isaca.org/Cobit/pages/default.aspx.

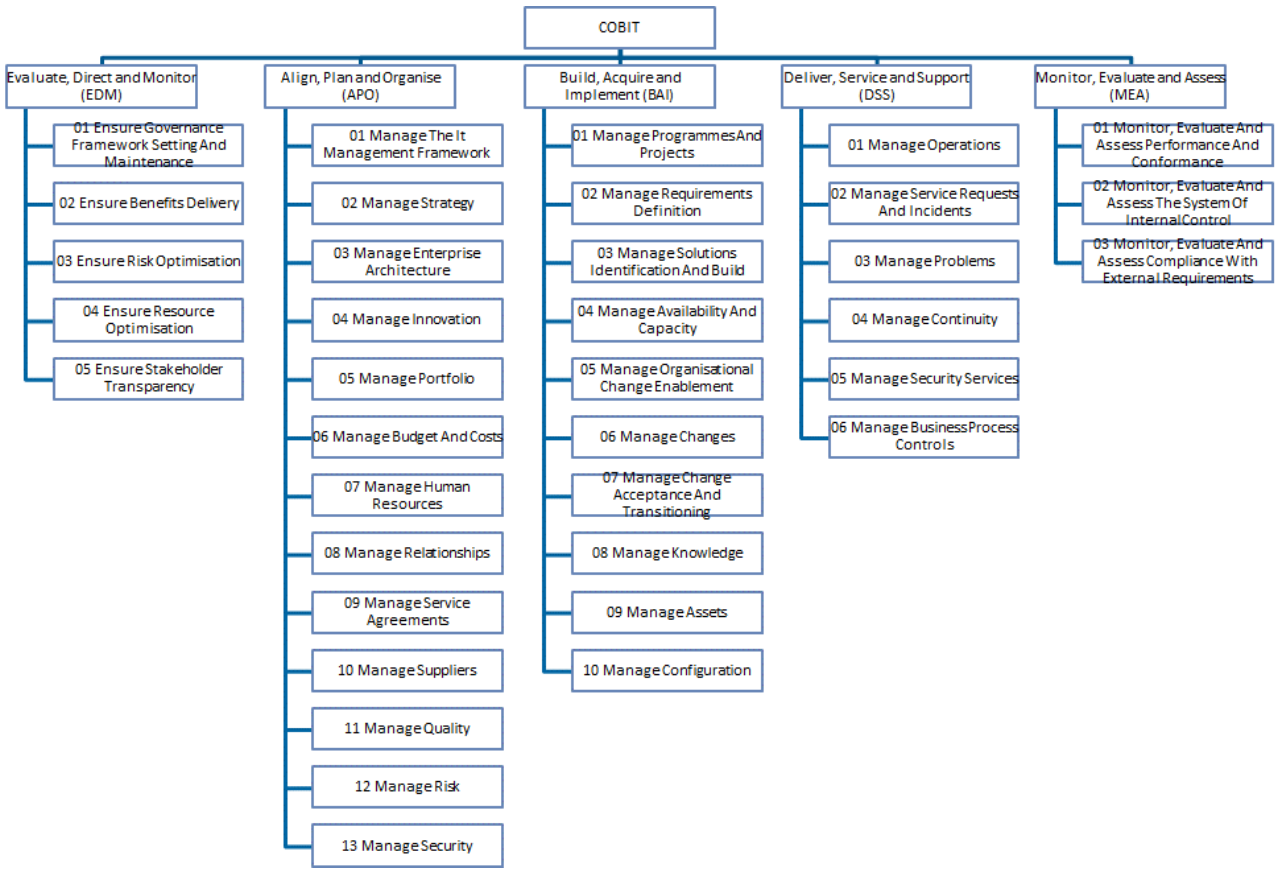
It started originally to assist financial auditors in addressing IT related issues and in putting control structures around IT. COBIT is currently a best-practices model for IT governance.

Data is a key resource for all organisations. From when it is created to the time that it is deleted or destroyed, technology plays a significant role in managing data. Information technology is increasingly advanced and has become pervasive in organisations as well as in social and public arenas. COBIT is a general IT governance framework that includes data specific-elements. This are incorporated into a wider IT view.

The COBIT governance model consists of the following areas:

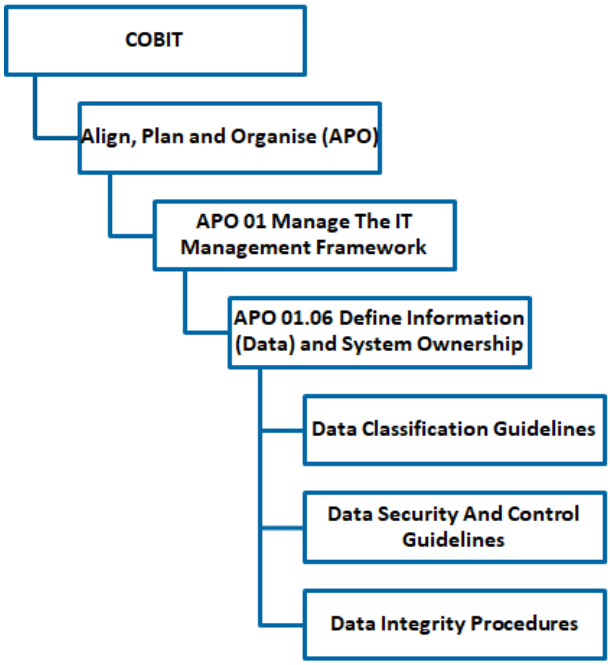
1. Evaluate, Direct and Monitor (EDM)
2. Align, Plan and Organise (APO)
3. Build, Acquire and Implement (BAI)
4. Deliver, Service and Support (DSS)
5. Monitor, Evaluate and Assess (MEA)

These are then sub-divided further into the following governance activity areas:



This structure is then further elaborated within the COBIT model. For example, within activity APO 01 there is a data-related activity called ***APO 01.06 Define Information (Data) and System Ownership*** that is concerned with the

- Definition and maintenance of responsibilities for ownership of information (data) and information systems
- Ensuring that owners make decisions about classifying information and systems and protecting them in line with this classification.



The following activities are performed to achieve this:

- Provide policies and guidelines to ensure appropriate and consistent enterprise-wide classification of information (data)
- Define, maintain and provide appropriate tools, techniques and guidelines to provide effective security and controls over information and information systems in collaboration with the owner
- Create and maintain an inventory of information (systems and data) that includes a listing of owners, custodians and classifications. Include systems that are outsourced and those for which ownership should stay within the enterprise
- Define and implement procedures to ensure the integrity and consistency of all information stored in electronic form such as databases, data warehouses and data archives

The full COBIT model is too detailed to describe here. The general principle is that there are existing well-defined and well-proven (data) governance frameworks that can provide a basis for the governance activities that can support GDPR implementation and operation.

8. Data Ethics

The increasing volume of personal data available and collected, both directly and indirectly – behaviour-type data – and associated data technologies – both data storage and data analysis tools and facilities - has extended the gap between what is possible in terms of personal data processing and what is should or legally can happen. The data collectors have substantial power and influence. The growth of free social media platforms means that information directly supplied and information derived from usage patterns is the commodity from which value can be obtained.

Data ethics is concerned with the study and assessment of moral problems related to (generally personal and possibly sensitive) data along its lifecycle from collection or generation to usage. It includes the use of data process algorithms to derive data products in relation to which there may be moral and ethical concerns. One objective of data ethics is to articulate and communicate what are morally good personal data processing solutions and approaches.

Data ethics is concerned with data consent, privacy, security and primary, secondary, tertiary and further uses.

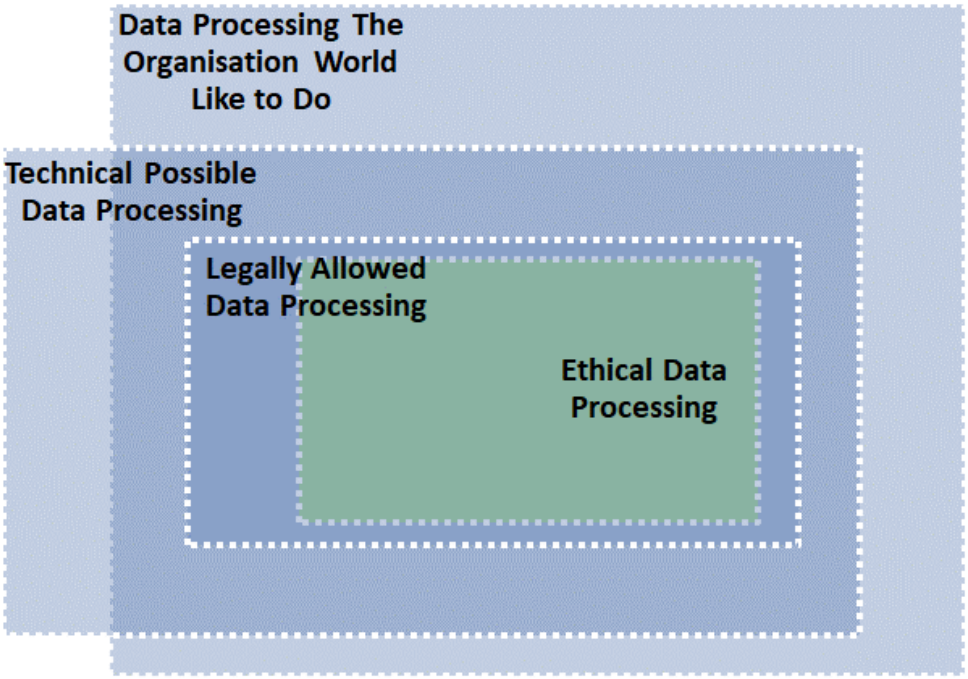
Data ethics issues now arise because:

- A very wide range of personal data is readily available from many sources
- The cost of integrating data from these many sources continues to fall
- The technical abilities to integrate, correlate and derive insight from these data sources are becoming readily and easily available
- Individuals, patterns of behaviour and insights about them can be identified very accurately
- The locations of individuals can be identified quickly and accurately
- Information can be collected, processed and results identified in real-time or near real-time

Schematically, in terms of personal data and its collection and processing there is:

- Data Processing The Organisation World Like to Do
- Technical Possible Data Processing
- Legally Allowed Data Processing
- Ethical Data Processing

There all represent decreasing sets of data and data processing activities.



Implicitly, GDPR is concerned with data ethics.

While data ethics is an abstract topic and far removed from the initial concerns of becoming compliant with GDPR is the face of business, technical and time challenges it one that will become more important over time.

I have mentioned it here to provide a wider and more jurisprudential context for GDPR.