General Data Protection Regulation (GDPR)

Odran Reid

May 2018

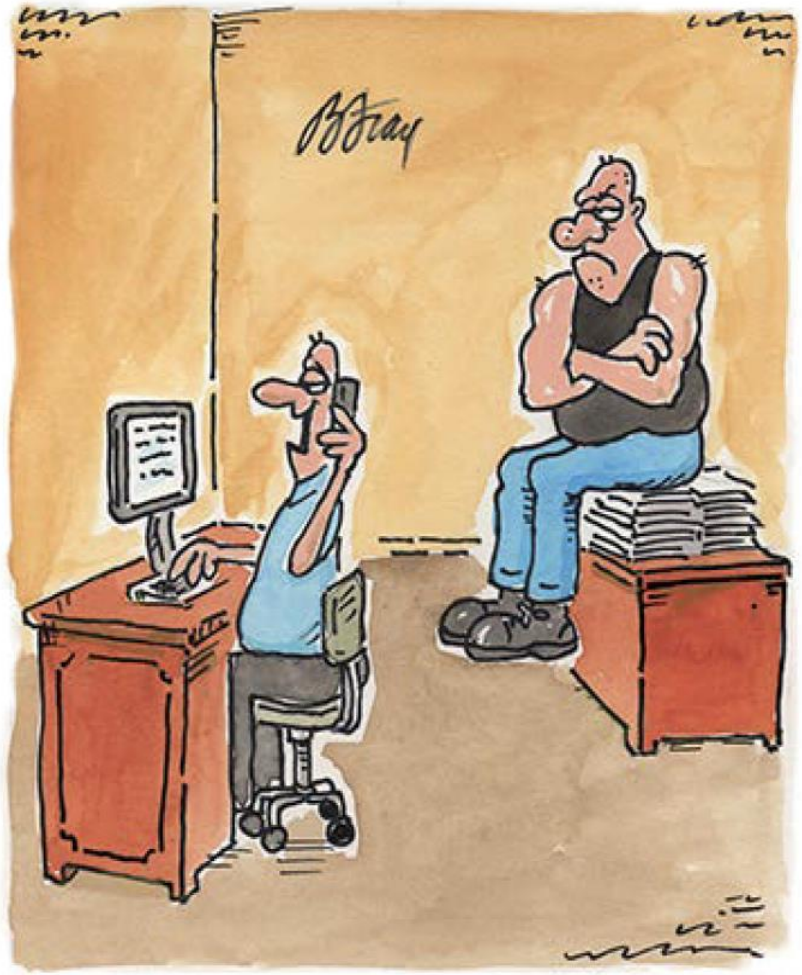
Today

- What is GDPR
- Data Protection and core Principles
- Rights of Individuals
- Data Protection Roles
- Consent - Explicit
- What you have to do
- What you do not have to do
- Data Breeches
- Good governance
- Preparing for the GDPR and showing compliance
- This is butchered from other peoples presentations

Frist Thing to Remember

- As it says on the Hitchhikers Guide to the Galaxy

- Don’t Panic



"I CAN ASSURE YOU THAT OUR CONCERN FOR PROTECTING PERSONAL INFORMATION IS VERY DEEP-SEATED!"

What is Data Protection

WHAT IS DATA PROTECTION?

As defined by the Data Protection Commissioner: “it is the safeguarding of the privacy rights of individuals in relation to the processing of their personal data.”

You share information about yourself with government bodies, banks, insurance companies, medical professionals and many others in order to avail of services or satisfy obligations. Organisations or individuals also obtain information about you from other sources. For the purpose of data protection such organisations or individuals who control the contents and use of personal data are know as data controllers

These rights apply where the information is held:

- ✓ electronically, or
- ✓ in a manual form, as part of a filing system that facilitates ready access to a specific individual’s information

RSM

CURRENT GOVERNING LEGISLATION

Data Protection Acts 1988 and 2003

At the moment, Irish data protection obligations are primarily governed by the Data Protection Act 1988 as amended by the 2003 Act. The act is governed by 8 principles:

1. Obtain and process the information fairly;
2. Keep it only for one or more specified and lawful purposes;
3. Process it only in ways compatible with the purposes for which it was given to you initially;
4. Keep it safe and secure;
5. Keep it accurate and up-to-date;
6. Ensure that it is adequate, relevant and not excessive;
7. Retain it no longer than is necessary for the specified purpose or purposes; and
8. Give a copy of his/ her personal data to an individual, on request.

THE 8 PRINCIPLES

1.Obtain and process the information fairly

- Personal data is obtained fairly if the data subject is:

✓ aware of the purpose for which the organisation in question is collecting the data at the point of collection and

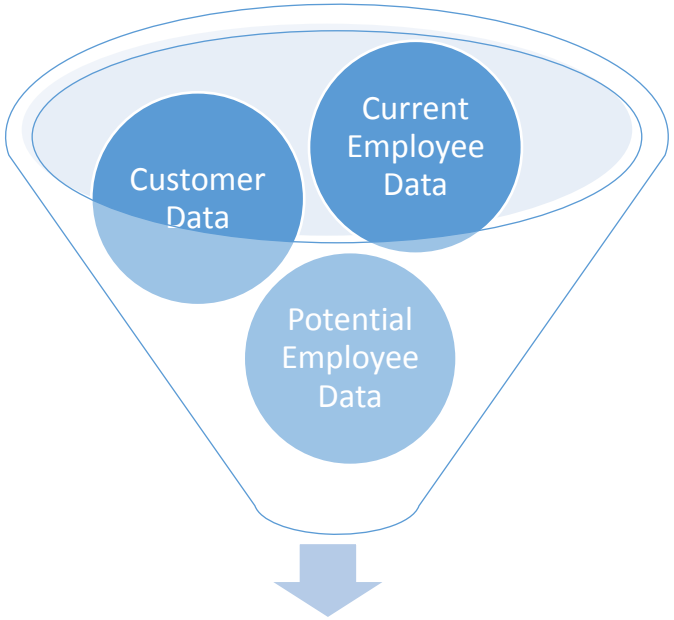
✓ aware of the categories of person/organisation to whom it may be disclosed.

- Many companies deal with:

✓ Employee data

✓ Customer/consumer/service user data

- Both groups must be fully informed as to why their data is being held and that it is being processed in a compliant manner.



Transparent data collection & usage process

RSM

THE 8 PRINCIPLES (CONT.)

- **2. Keep it only for one or more specified and lawful purposes**
- Collected data – from customers and employees – must be used for the purpose it was collected:

THE 8 PRINCIPLES (CONT.)

- **3. Process it only in ways compatible with the purposes for which it was given to you initially**
- Do not disclose any personal data to any third party without the consent of the data subject. Personal data of employees should not be disclosed to work colleagues unless they have a legitimate interest in the data in order to fulfil official duties.
- However there are certain exceptions to this rule:

At the request or with the consent of the data subject or a person acting on his/her behalf

Where the data subject has already been made aware of the person/organisations to whom the data may be disclosed

Required for the purposes of preventing, detecting or investigating offences, prosecuting offenders or assessing moneys due to the state

Required by a court order, for legal advice or proceedings

Authorized for safeguarding the security of the State

Required urgently to prevent injury or damage to health or serious loss or damage to property

Required to protect the international relations of the State

THE 8 PRINCIPLES (CONT.)

- **4. Keep it safe and secure**
- The organisation handling the data must ensure that the right and safe storage channels are used to avoid inadvertent destruction, amendment, loss, disclosure, corruption or unlawful processing:

Personal data should be subject to stringent controls, passwords, back-ups and access log

Screens and files showing personal data should not be visible to unauthorized individuals

Special care must be given to mobile or tablet devices

Manual data should be kept in locked rooms or cabinets

The Data Controller, in disclosing personal data to a Data Processor should only do so under a written agreement, specifying the security arrangements which must be in place.

THE 8 PRINCIPLES (CONT.)

- **5. Keep it accurate and up-to-date**
- Data Subjects can inform the organisation handling the data if there are any changes or errors with the data. The organisation will have to amend the data accordingly.

- **6. Ensure that it is adequate, relevant and not excessive**
- Obtain personal data only when there is a clear purpose for doing so, obtain only that which is necessary for fulfilling that purpose and ensure that it is used only for that purpose.

THE 8 PRINCIPLES (CONT.)

- **7. Retain it no longer than is necessary for the specified purpose or purposes**
- Data should not be kept for any longer than is necessary for the purpose for which it was collected and should not be subject to further processing that is not compatible with that purpose.
- Personal data should be disposed of securely when no longer required. The method should be appropriate to the sensitivity of the data (shredding or incineration is appropriate in respect of manual data; and reformatting or overwriting in the case of electronic data).

8. Provide a copy of his/her personal data to an individual, on request

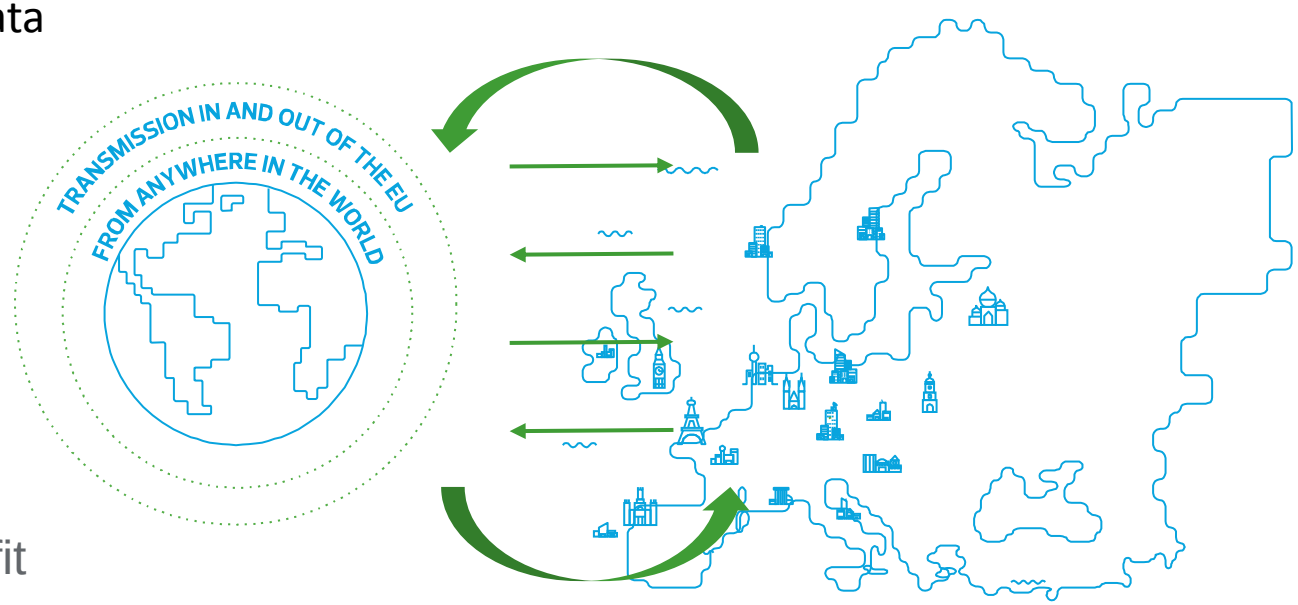
Upon submitting a written request, the data subject has the right to a copy of the information that an organisation holds about them, subject to certain restrictions. that do exist.

WHAT IS THE GDPR?

- The **General Data Protection Regulation** (GDPR) will come into force on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

- The GDPR emphasises transparency, security and accountability by data controllers and processors, while at the same time standardising and strengthening the right of European citizens to data privacy.

- Companies, government agencies and non-profit organisations who interact with personal identifiable data of EU citizens have until 25 May when GDPR comes into force to comply.



RSM

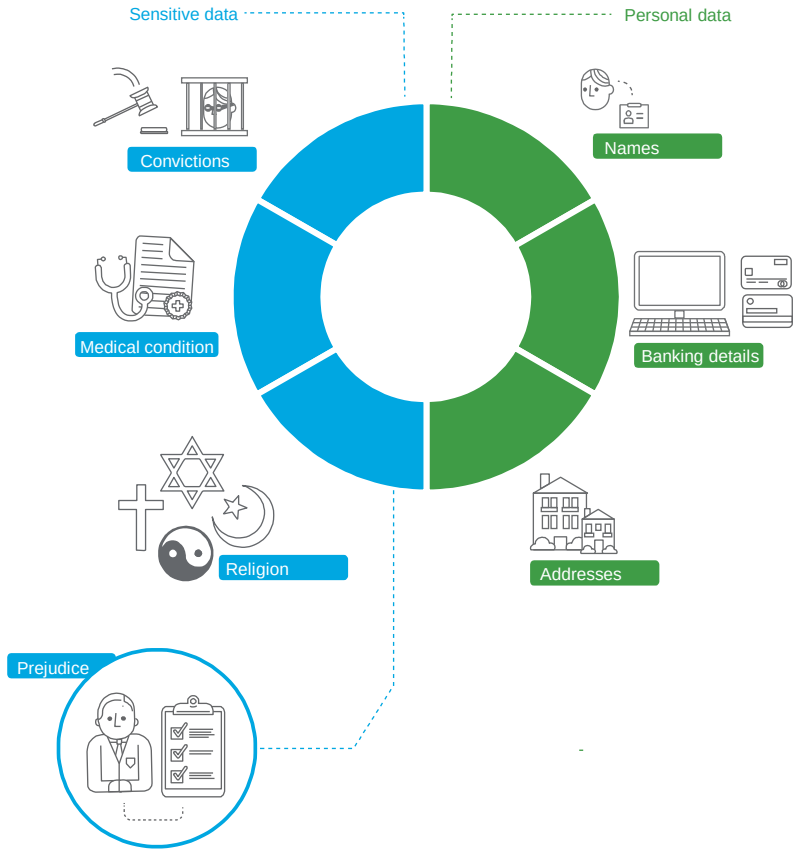
The GDPR in Context

- It heightens accountability for how personal data is acquired and handled

- •It gives **EU residents** more control over their personal data

- •It applies to sole traders and organisations established in the EU/EEA and to those outside of the EU that process the personal data of EU residents (including cloud computing service providers).

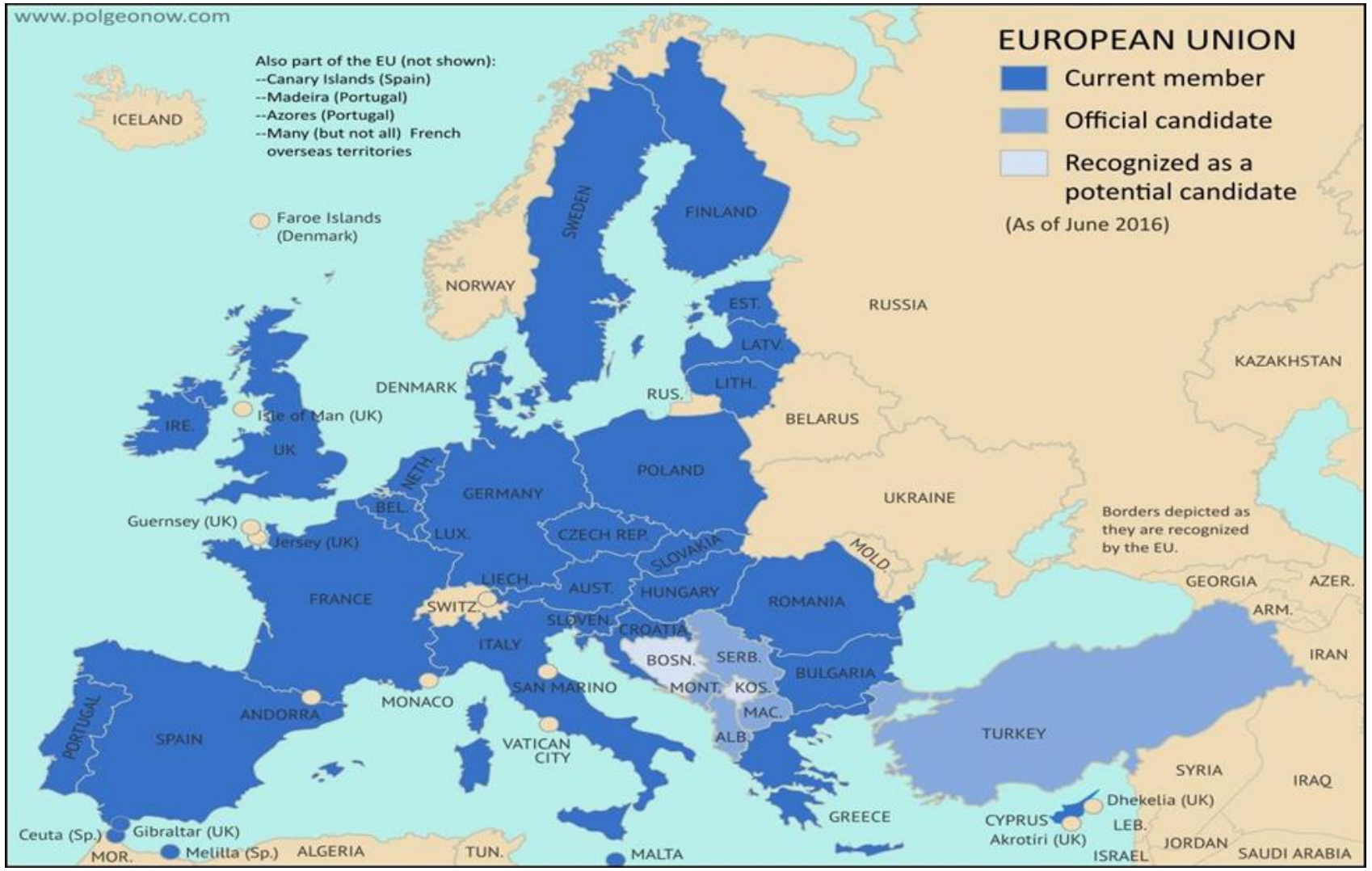
SENSITIVE PERSONAL DATA



Sensitive personal data is a special category of personal data.

These require a higher standard of care by the GDPR.

GDPR - SCOPE


www.polgeonow.com
EUROPEAN UNION
Current member
Official candidate
Recognized as a potential candidate
(As of June 2016)
Also part of the EU (not shown):
--Canary Islands (Spain)
--Madeira (Portugal)
--Azores (Portugal)
--Many (but not all) French overseas territories
ICELAND
Faroe Islands (Denmark)
NORWAY
SWEDEN
FINLAND
RUSSIA
EST.
LATV.
LITH.
KAZAKHSTAN
DENMARK
RUS.
BELARUS
IRE.
Isle of Man (UK)
UK
NETH.
GERMANY
POLAND
BEL.
LUX.
UKRAINE
Guernsey (UK)
Jersey (UK)
CZECH REP.
SLOVAKIA
MOLD.
Borders depicted as they are recognized by the EU.
FRANCE
LIECH.
AUST.
HUNGARY
ROMANIA
GEORGIA
AZER.
ARM.
SWITZ.
SLOVEN.
CROATIA
ITALY
IRAN
BOSN.
SERB.
BULGARIA
SAN MARINO
MONT.
KOS.
MONACO
MAC.
ANDORRA
PORTUGAL
SPAIN
ALB.
TURKEY
VATICAN CITY
SYRIA
IRAQ
Dhekelia (UK)
GREECE
CYPRUS
Akrotiri (UK)
LEB.
Ceuta (Sp.)
Gibraltar (UK)
JORDAN
MOR.
Melilla (Sp.)
ALGERIA
TUN.
MALTA
ISRAEL
SAUDI ARABIA

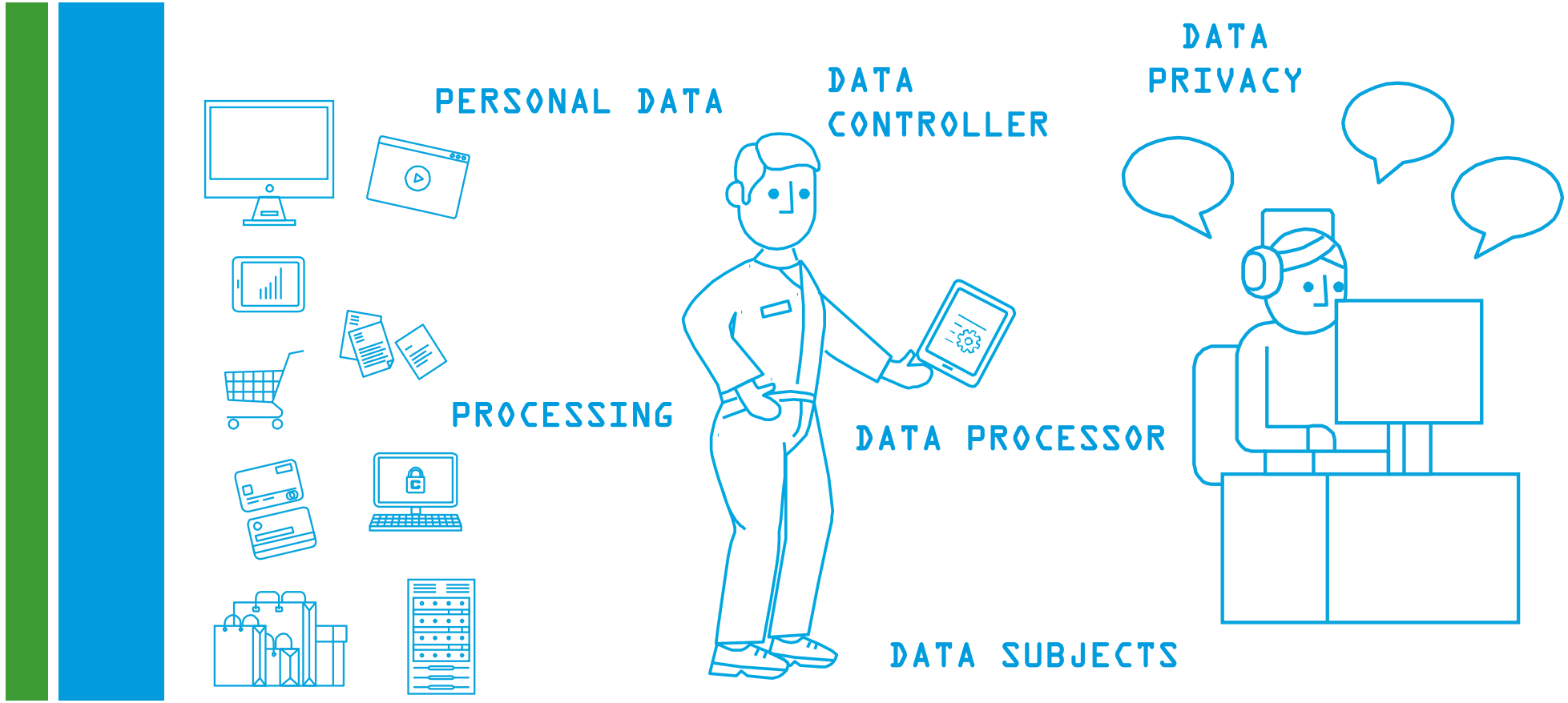
SO WHO HAS TO COMPLY?

An organisation has to comply if:

They control or process the personal data of EU residents

This applies irrespective of where the organisation is based.

GDPR TERMINOLOGY



The GDPR -Terminology

Personal Data

- Any information relating to an identified or identifiable natural person. Examples of personal data include a person's name, home address, photo, an email address, bank details, posts on social networking sites and medical records.

The GDPR -Terminology

Sensitive Personal Data

- The GDPR applies to sensitive personal data, which it refers to as "special categories of personal data". These special categories of sensitive data include data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, genetic data and biometric data.

Processing

- Applies to both automated personal data and to manual filing systems where personal information is accessible according to specific criteria.

The GDPR -Terminology

Data Controller

- A data controller is a person, organisation, company or legal entity who controls and is responsible for keeping and the use of personal data on computer or in structured manual files. Examples of data controllers would be pharmacists and General Practitioners.

Data Processor

- A data processor is a person, organisation, company or legal entity who processes personal data, but does not exercise responsibility for or control the personal data. Examples of data processors would include payroll companies, market research companies and accountants.

GDPR –Clarify Processing Activity

- **Commercial/operational activity**: examples of types of processing you conduct
  - **Recruitment**: how people apply for jobs, online, email, snail mail
  - **Employment**: paying salaries, attendance record, PAYE, paying expenses, personnel files, appraisals, grievances
  - **Workplace**: CCTV, accident reporting, issuing security cards
  - **Communications**: signing up for newsletters & direct mail
  - Anything else? List the types of personal data in your organisation.

Data Journey –Map

- All points of contact with the data subject where personal data is captured or recorded
- All staff members and third parties who have access to data subjects' personal data at any stage
- All locations (both digital and physical) where personal data is stored
- Methods and procedures used to safeguard personal data during collection, processing, storage and deletion

Practical Exercise

1. Can you identify the ‘data journey’ in your organisation? What are the steps or stages in the journey?

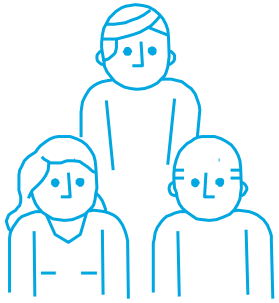
2. What are the implications of the data journey from a data processing, cyber security and human error perspective?

NEW CONCEPTS AND KEY PRINCIPLES

Explicit consent

Contracts

PIAs



Individual rights

Breach notice

Incident register

GDPR -Five Key Steps to Data Safety 1

1. **Identify the data you process and store**
   - What Personal Data do you collect and process?
   - Is the data accessible without the consent of the data subject? (how did you get the data)
   - Is the data forwarded to a third party? If so, make sure that agreements with them identify them as data processors.
   - If data processors are outside of the EEA, you may need an additional contract to enable you to send the data to the country or supplier.

GDPR -Five Key Steps to Data Safety 2

2. Create your data purpose(s)

- If you already have a stated data purpose, then make sure it is up-to-date i.e.:
  - What data is collected
  - Why it is collected
  - How it is processed, by whom and where (within/outside EEA)
  - How long it will be retained for
  - Who to contact in case of a data protection query

GDPR -Five Key Steps to Data Safety 3

3. Ensure Consent

- Make sure you are obtaining the Data Subject's consent to use their personal data
- Record their consent(s). Be able to demonstrate consent to the Data Subject or the Data Protection Commissioner (Subject Access Request or complaint)
- Where existing data has no record of consent for it, you may want to look at actively re-establishing consent. In some cases (such as in the provision of an active service) consent may be implied, but this point should be considered.

GDPR -Five Key Steps to Data Safety 4

4 Support the data subjects’ rights

- Check that your internal processes, procedures and computer systems are able to support a Data Subject's rights within the time frames dictated by the GDPR.

GDPR -Five Key Steps to Data Safety 5

5. Create an incident response plan

- If a data breach occurs, ensure that an Incident Response Plan is in place to guide the process that will enable the correct response to be made.

- Following the discovery of a data breach incident involving personal data the Data Protection Commissioner or the Data Subject will be informed as to the nature and scale of the breach, the action that has been taken, the potential impact on the Data Subjects, and all within 72 hours of the discovery of the breach!

Methods of Demonstrating Compliance

- ***Documentation***
  - Organisations should maintain relevant documentation concerning its data processing activities. Organisations must record the following information:
  - Name and details of the organisation. Where applicable the name(s) and detail(s) of other data controllers, data protection officer and representative(s) should also be recorded.

- Name and details of the organisation. Where applicable the name(s) and detail(s) of other data controllers, data protection officer and representative(s) should also be recorded.
  - Purpose of the data processing
  - Description of the catagories of individuals and categories of personal data being processed
  - Details of transfers to third countries and clear documentation of the mechanisms in place to safeguard data transfer.
  - Data retention schedules
  - Description of technical and organisational security measures

Methods of Demonstrating Compliance

Technical and Organisational Measures

- Organisations should review and update data protection policies as necessary, train staff (and volunteers), address human resources implications of the GDPR and conduct an audit of data processing activities, with a view to amending and updating data processing activities.

Data Protection by Design

- In developing data processes, organisations should design implementation of the principles into data processes early on, particularly with respect to data minimisation, transparency, pseudonymisation, storage limitation, security features and the ability of individuals to monitor data processing.

Methods of Demonstrating Compliance

Data Protection by Default

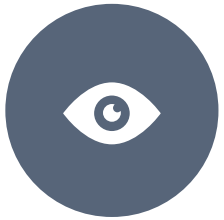
- Organisations should ensure that default service settings are data protection friendly for individuals.

Data Protection Officer

- Where appropriate, appoint a Data Protection Officer (DPO). A DPO must be appointed if an organisation is:
  - A public authority (except for courts acting in their judicial capacity)
  - carrying out large scale systematic monitoring of individuals e.g. online behaviour tracking
  - carrying out large scale processing of special categories of data or data relating to criminal convictions and offences

What are the key changes with the GDPR?

Personal Privacy



Individuals have the right to:

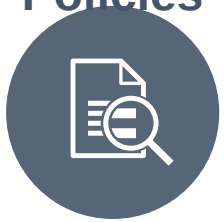
- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data

Controls and Notifications

companies are required to:

- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies

Transparent Policies



companies will need to:

- Train privacy personnel & employee
- Audit and update data policies
- Employ a Data Protection Officer (for larger organizations)
- Create & manage processor/vendor

Training and Governance

companies need to:

- Protect personal data using appropriate security practices
- Notify authorities within 72 hours of breaches
- Receive consent before processing personal data
- Keep records detailing data processing

Approach to Compliance

Complete

- Identified areas where client information is stored
- Started raising staff awareness through communications
- Developing a Plan to centralise Personal Data to simplify governance.

KEY CHANGES – MORE INFORMATION REQUIRED

Details of their purpose and legal basis for processing data

How long data will be retained and any transfers outside the EU

Individuals can complain to local regulatory bodies if they are dissatisfied with how their data is handled

ACTION: Privacy/fair processing notices or other communications should be reviewed and amended to meet the new requirements. Information should be provided in concise, easy to understand and clear language.

KEY CHANGES - CONSENT

Consent must be "freely given, specific, informed and unambiguous"

Consent may be withdrawn at any time

Consent cannot be inferred e.g. pre-ticked boxes or inactivity

ACTION: Procedures to obtain and record consent should be reviewed to check they are in line with the new GDPR requirements.

KEY CHANGES – INDIVIDUAL RIGHTS

Right to be forgotten (have personal data removed from systems or online content)

Right to data portability (have data provided electronically in commonly used format)

Right not to be subjected to automated data profiling (where this would produce a legal effect)

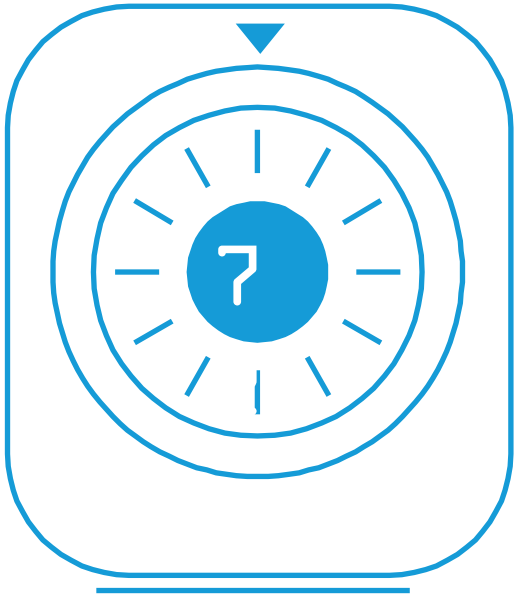
ACTION: Ensure that processes are in place to respond in a consistent and timely manner to customers who assert these enhanced rights.

KEY CHANGES – INDIVIDUAL RIGHTS

Right to request that organisations erase personal data without undue delay where:

- it is no longer necessary for the purpose it was collected
- the data subject withdraws consent and there is no other legal ground for processing
- the data subject exercises their right to object and there is no overriding legitimate ground for processing
- the processing is unlawful

BREACH NOTIFICATIONS



- Organisations are now under legal obligation to notify local authorities within 72 hours if EU resident data is lost.
  - Only exception is if the data was encrypted.
  - Organisations have to inform individuals if an “adverse impact” is determined from the breach.
- Service providers (data processors) now have obligations to data controllers.

Penalties for non-compliance

If organisations do not comply, they face a maximum fine of:

Other consequences – reputational damage, financial loss, litigation etc.

Examples of penalties

- **Uber**
  - Admitted it paid hackers responsible for a data breach $100,000 (€84,790) not to disclose the data breach to authorities.
  - November 2017

- **Carphone Warehouse**
  - Fined **£400,000** after serious failures placed customer and employee data at risk.
  - 10th January 2018

- **Department of Social Protection**
  - A civil servant who sold personal data of citizens to private investigators working for insurance companies was jailed.
  - 26th January 2018

HOW TO PREPARE FOR THE UPCOMING GDPR

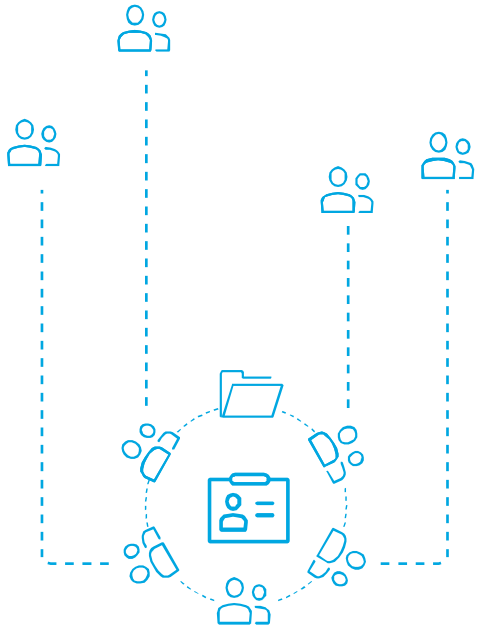
KEY ACTIVITIES

Carry out an information audit and data flow mapping exercise

Update all policies and procedures to reflect changes

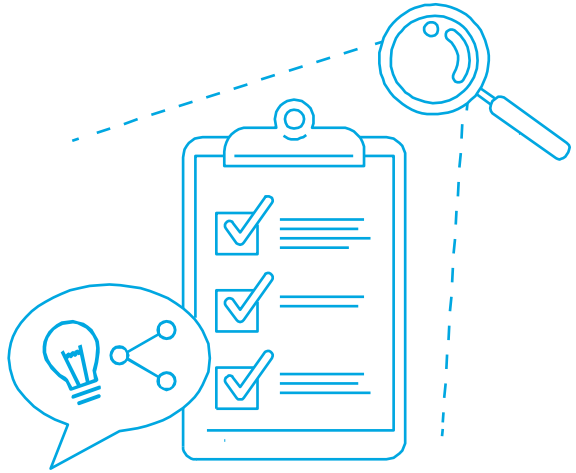
Reviewing data-related service provider contracts to reflect impact of the GDPR on controller and processor obligations

KEY ACTIVITIES



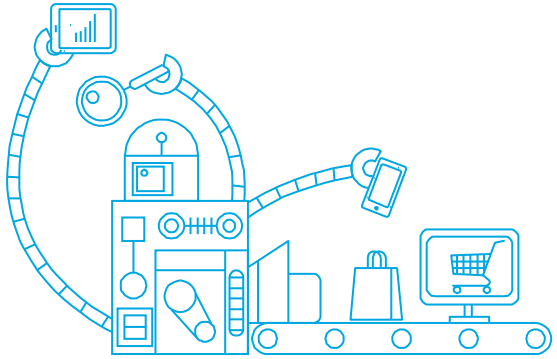
Form a data governance group

Implement / review breach notification procedures and Incident Management Plans

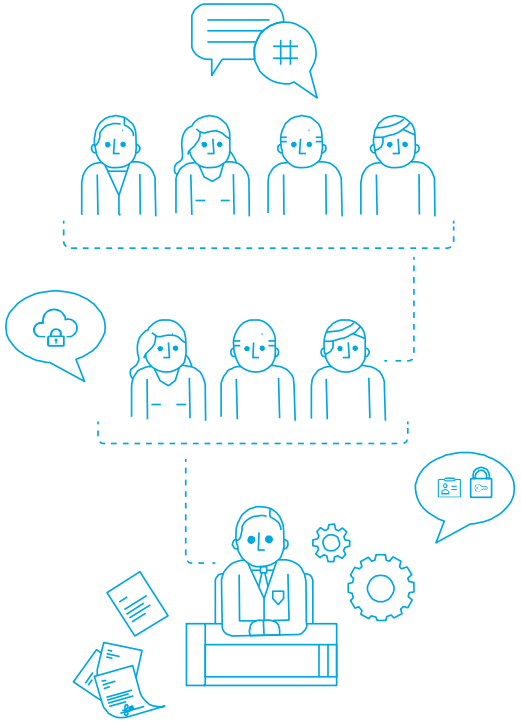


Review impact of GDPR on data retention policies e.g. on archiving

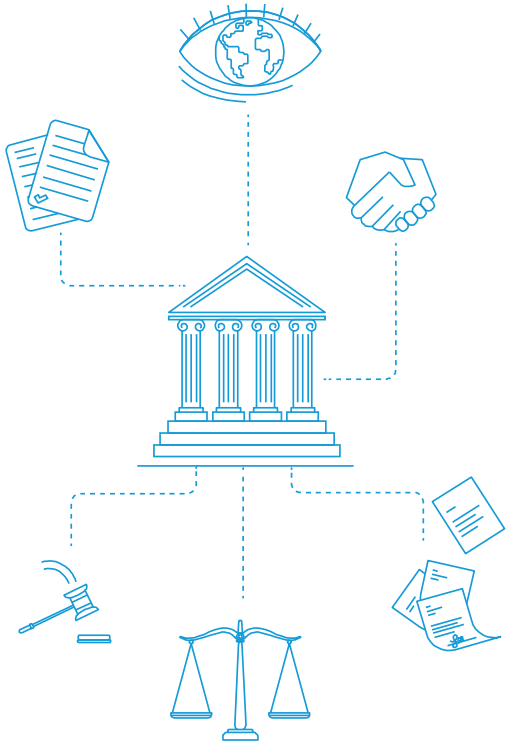
KEY ACTIVITIES



Review IT development and purchase procedures – ‘Privacy by Design’



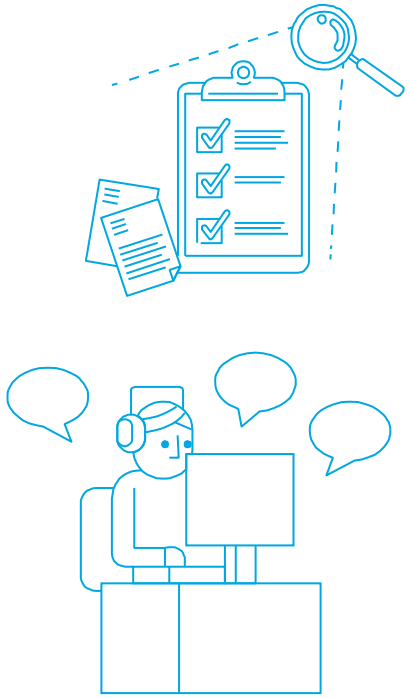
Consider the position of the existing DPO within the management structure



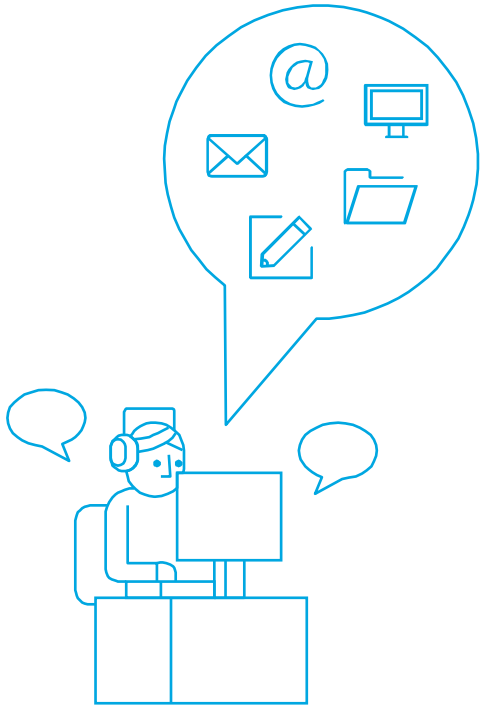
Consider and record lawful bases for processing

KEY ACTIVITIES

Create and maintain an information asset register



Check accountability for data governance is clear and precise

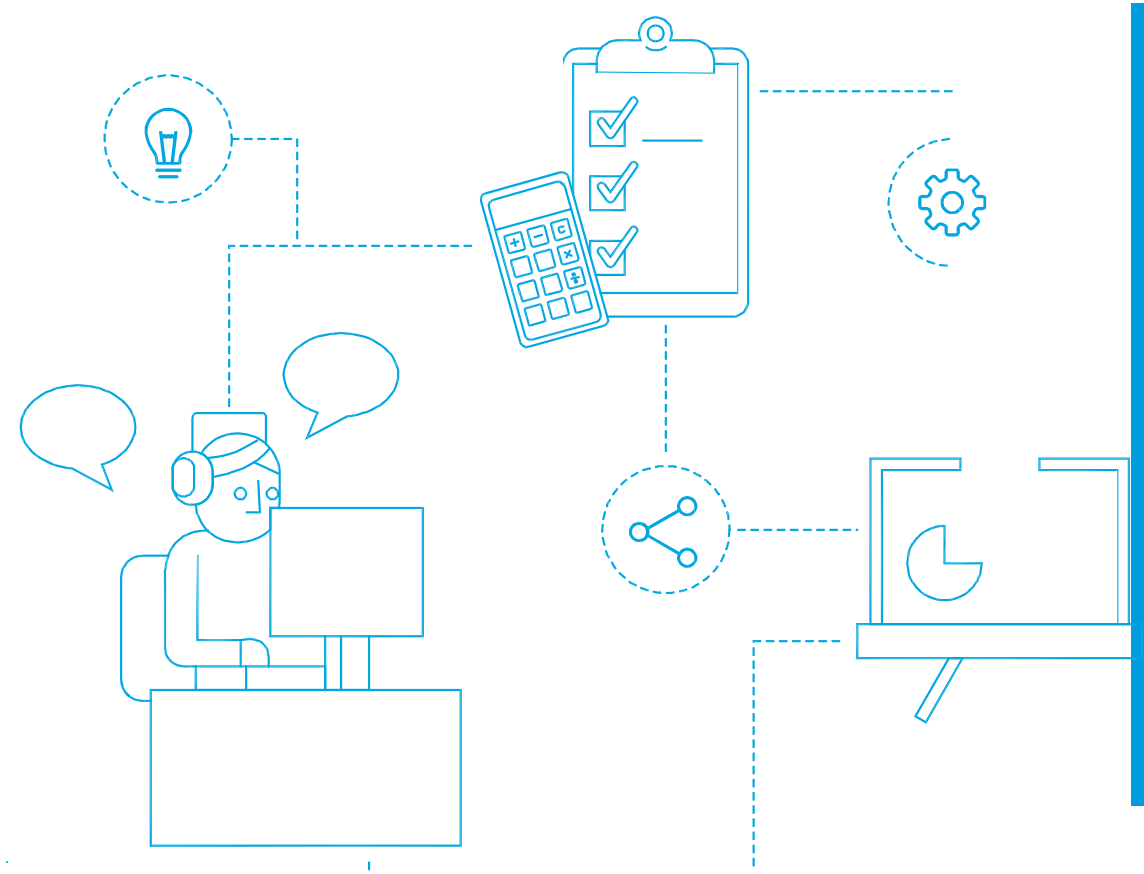


Check how consent is obtained. Are changes to this process required?
Retain records of consent

GDPR ROADMAP TO COMPLIANCE

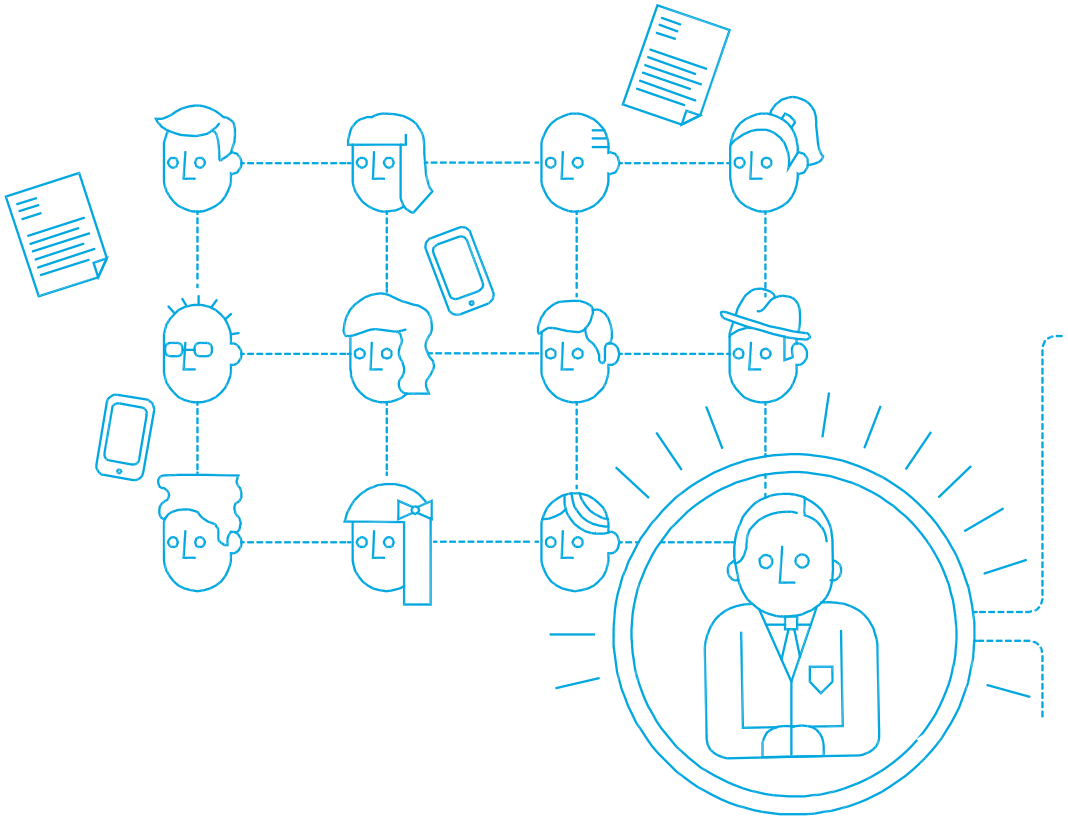
RSM

MOBILISATION



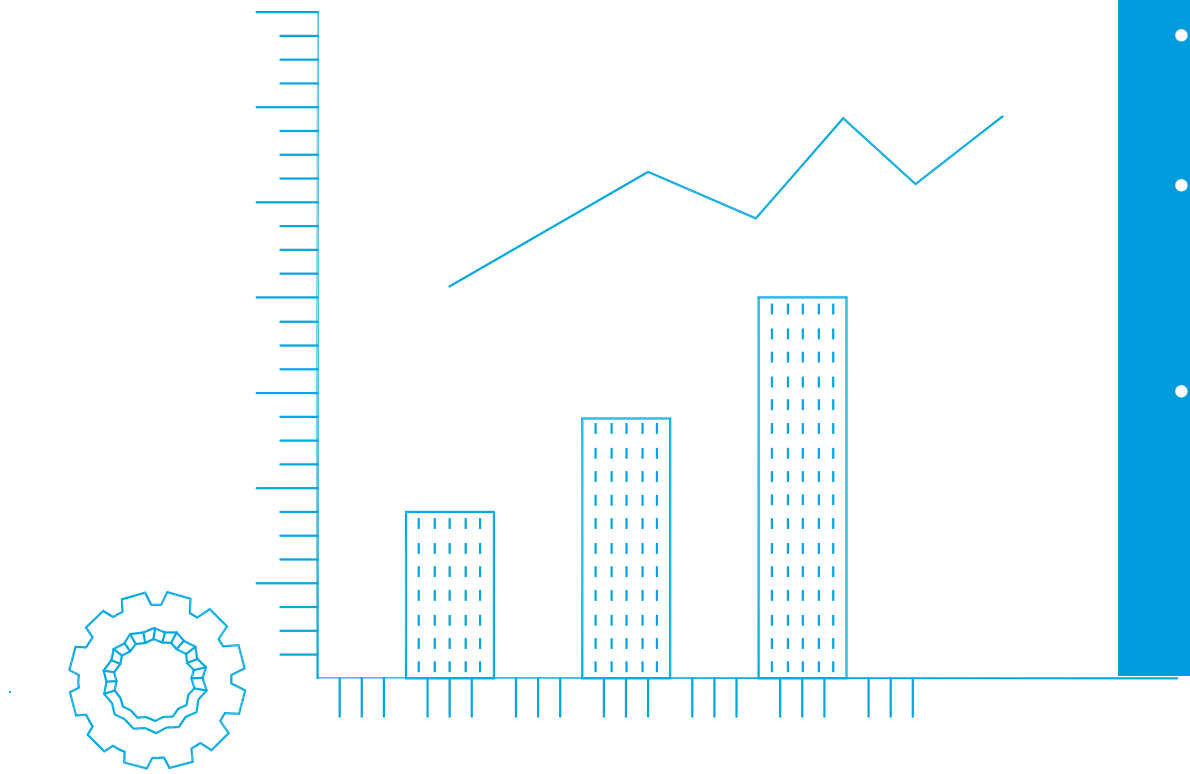
- Critical first phase
- Define scope
- Expected outputs
- Agree plan
- Commit resources
- Establish governance
- Create PID or Charter

DISCOVERY



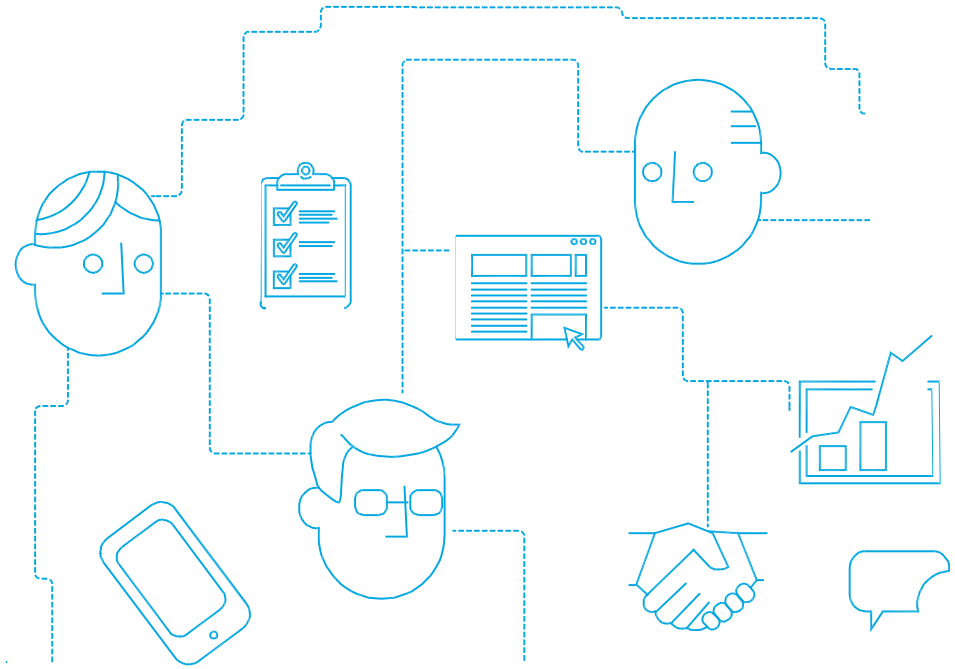
- Review documentation
- Interviews
- Review policies & procedures
- Discuss functionality of systems to meet the GDPR requirements

ANALYSIS



- Analysis and evaluation
- Processes and policies in place
- Identification of missing policies and measures in order to comply
- Assistance in implementing the processes, procedures and policies to comply

REPORTING



- Concise report
- Finalised post-client feedback
- Focus on key findings in gap analysis
- Recommendations reflected in budgeted roadmap to compliance

THE NEW IRISH DATA PROTECTION BILL

RSM

NEW IRISH DATA PROTECTION BILL

- Ireland's new Data Protection Bill was published on 1st February 2018.
- The new bill transposes much of the GDPR text directly and addresses the powers of the Data Protection Authority.
- The Bill will establish a Data Protection Commission in place of the current Office of the Data Protection Commissioner (ODPC)
- A controversial inclusion in the Bill is the exemption of Public Bodies from the administrative fine regime, except where acting as an "undertaking", (i.e. providing goods or services for gain)
- The existing 1988 Act is not repealed but amended, meaning that three Data Protection Acts will then be in force – an amended 1988 Act, the 2003 Amendment Act and the 2018 Act

CONSENSUS ORIENTED
PARTICIPATORY
ACCOUNTABLE
FOLLOWS THE RULE OF LAW
GOOD GOVERNANCE
TRANSPARENT
EFFECTIVE AND EFFICIENT
RESPONSIVE
EQUITABLE AND INCLUSIVE

What to Audit?

I.T. Personnel

- Who is responsible for implementing data and cyber security in the company? What level of training have they received in the last two years of relevance to their roles?

- Does the company have an I.T. Strategic Development Plan?

- Asset Management
- Is an up-to-date asset management policy in place?

What to Audit?

Wireless Networks

- Are wireless networks appropriately secured?

- **Operating Systems**
- Are operating systems and software efficacy reviewed on a scheduled basis?

What to Audit?

Filtering Software

- Is email and internet traffic filtering software in place?

Servers

- Is a list of servers available and the names of the people who are responsible for checking that servers are up-to-date?

Firewalls?

- Are appropriate firewalls and intrusion detection software in place?

Configuration Management

- Is appropriate configuration management in place?

What to Audit?

- **Security Scans - regular**
- **Anti-virus Software – is it in place and up to date**
- **Backups – are they scheduled?**
- **Encryption – are your files encrypted**
- **Lap tops and portable devices**
- **USB drives - what is your policy?**
- **Log Files – so they are reviewed for relevance**
- **E mailing personal information – what is your policy?**
- **Classification of data**
- **Who has access to what data and why?**

GDPR myths

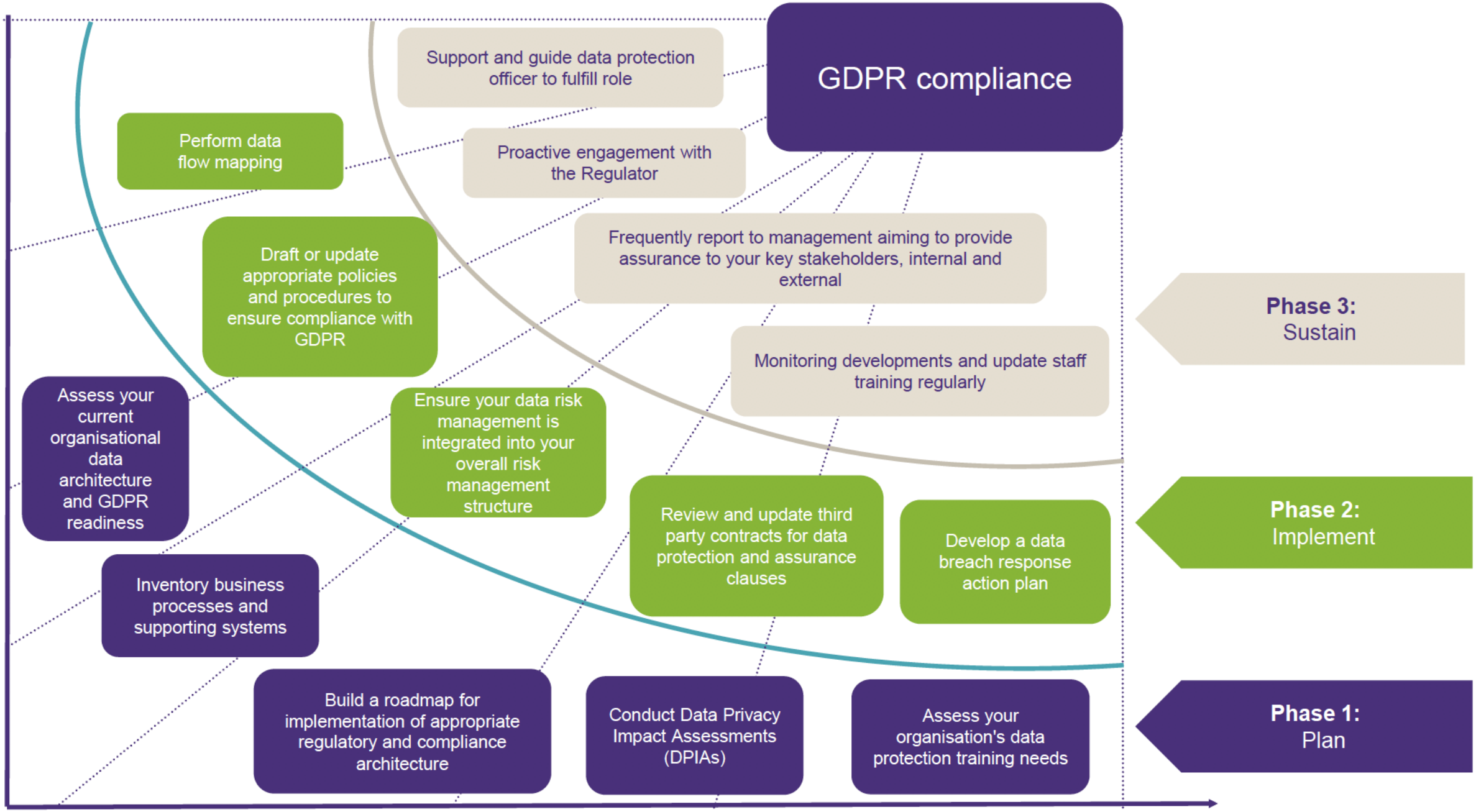
- This doesn’t apply to me!
- I already have IT security
- I have loads of time
- I’m only a data processor

Expectation on outcome

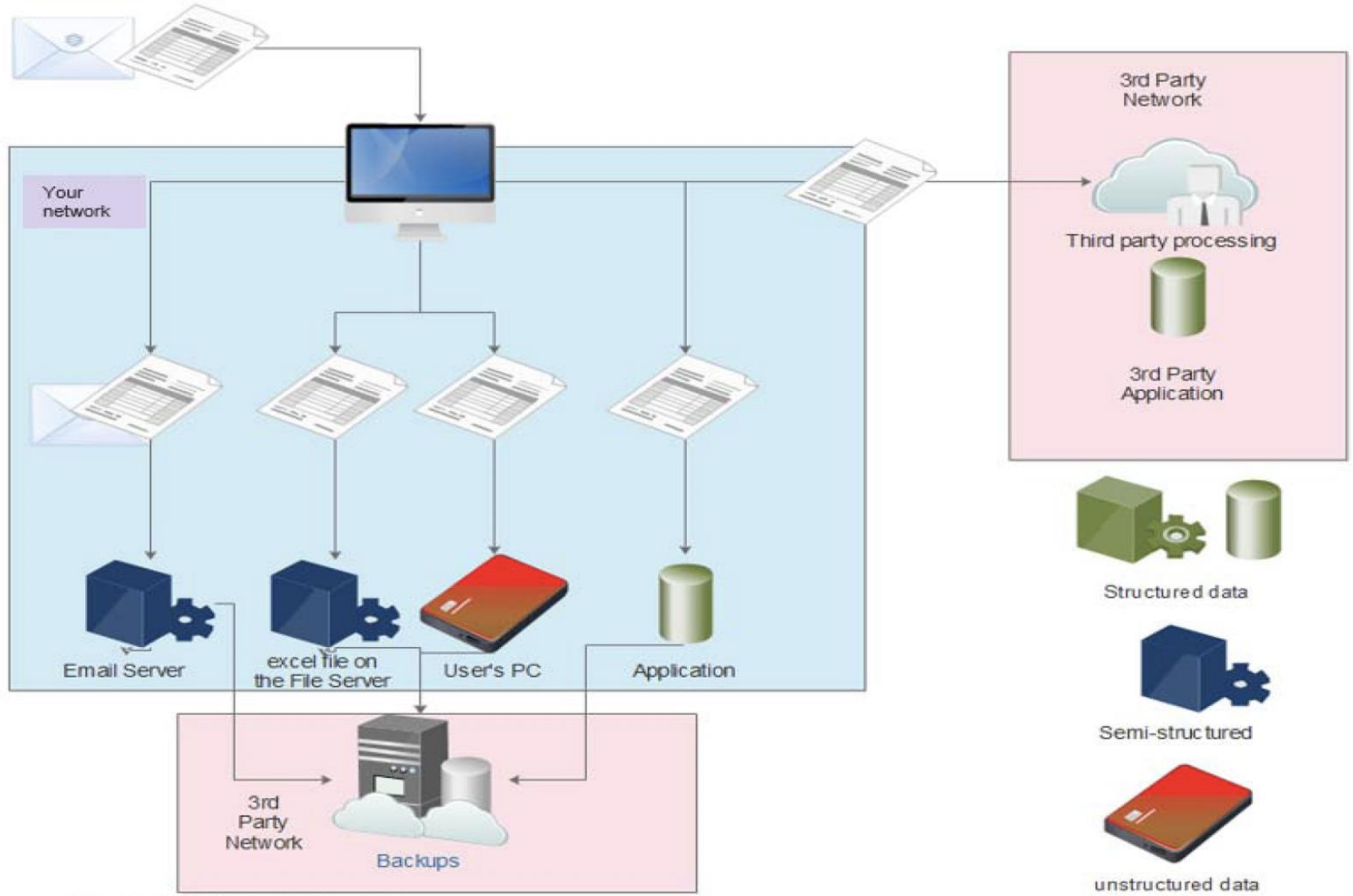
Assess GDPR readiness and developing an implementation plan

Implement the privacy programme based on the plan

Sustain the privacy practice in compliance with EU GDPR regulations


GDPR compliance
Support and guide data protection officer to fulfill role
Perform data flow mapping
Proactive engagement with the Regulator
Draft or update appropriate policies and procedures to ensure compliance with GDPR
Frequently report to management aiming to provide assurance to your key stakeholders, internal and external
Monitoring developments and update staff training regularly
Phase 3: Sustain
Assess your current organisational data architecture and GDPR readiness
Ensure your data risk management is integrated into your overall risk management structure
Review and update third party contracts for data protection and assurance clauses
Develop a data breach response action plan
Phase 2: Implement
Inventory business processes and supporting systems
Build a roadmap for implementation of appropriate regulatory and compliance architecture
Conduct Data Privacy Impact Assessments (DPIAs)
Assess your organisation's data protection training needs
Phase 1: Plan

Data inventory



Data distribution and replication