ARE YOU READY TO MEET THE CHALLENGES OF GDPR?

A ROADMAP TO COMPLIANCE

Who we are

Michael Shatter

National Director, Security and Privacy Risk Services, Risk Advisory, RSM Australia

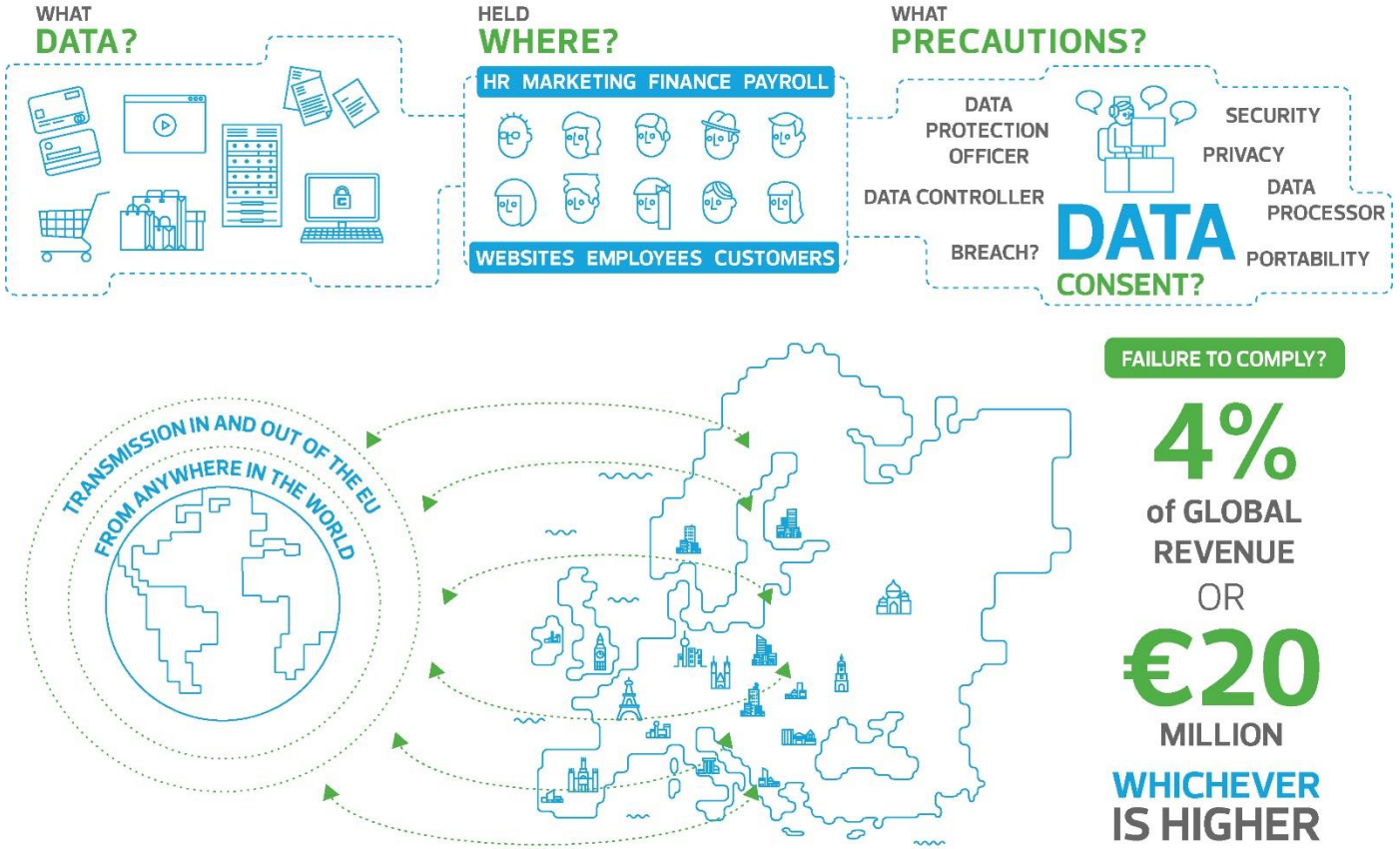
Has over 24 years' experience, specialising in the delivery of IT Security & Privacy Services. He has worked on an extensive range of large and complex projects ranging from security reviews of mainframe computer systems through to multinational cyber security reviews and risk assessment in both public and private sectors.

Jaime Lam

Principal, Risk Advisory, RSM Australia

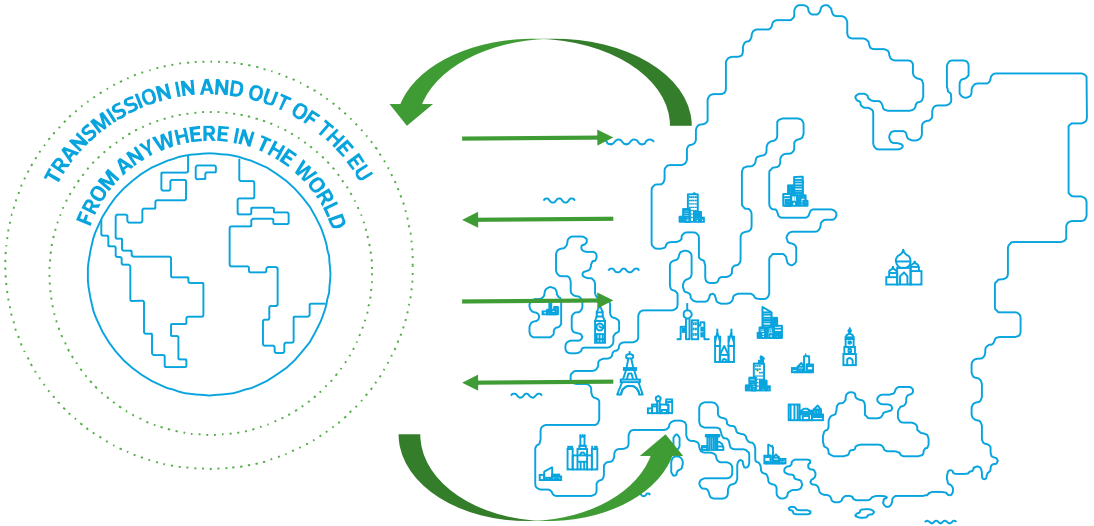
Has over 12 years' experience in both private and public sector entities and is responsible for delivery of SOX engagements, risk management and corporate internal audit reviews. As an ISACA member, she has experience in the assessment of IT controls. Jaime has also worked with many international clients around the Asia Pacific region.

ARE YOU READY TO MEET THE CHALLENGES OF GDPR?



What is the GDPR?

- European Union General Data Protection Regulation – “EU GDPR.”
- New data protection law adopted by the EU in April 2016, intended to bolster data privacy protections for EU residents.
- 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



The GDPR terminology

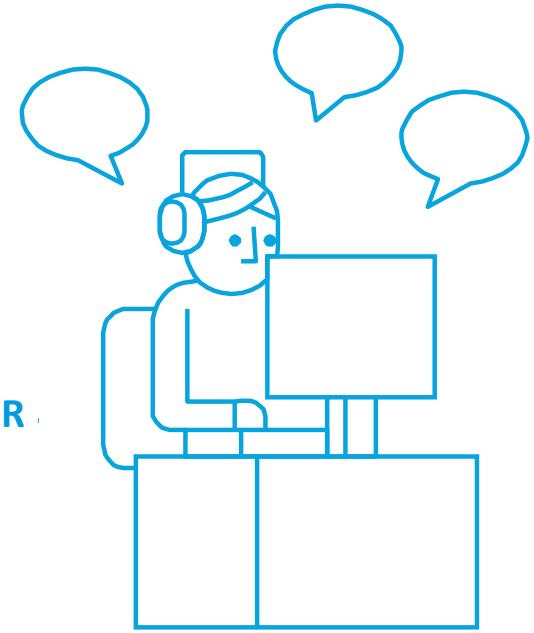
PERSONAL DATA

PROCESSING

DATA CONTROLLER

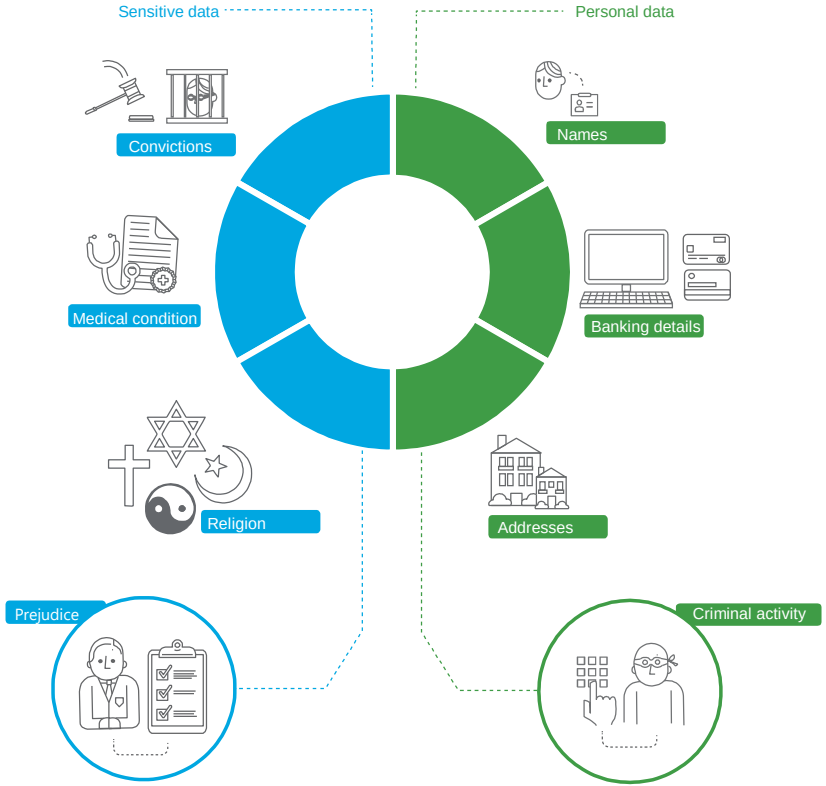
DATA PROCESSOR

DATA SUBJECTS



NOTIFICATION

Sensitive personal data



Sensitive personal data is a special category of personal data.

These require a higher standard of care by the GDPR.

So who has to comply?

Compliance is **mandatory** if either of the following statements are true:

You have controllers or processors of personal data based in the EU

You process the personal data of EU residents (regardless of where you are based)

GDPR – Asia Pacific Considerations

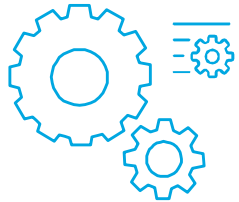
- **Singapore –** As of 25th January 2018 Currently, there are no mandatory requirements under the Act for data users to notify the Commission or individuals regarding data protection breaches in Singapore. There are however draft proposals to introduce mandatory data breach notifications in Singapore. Organisations are advised to monitor developments.
- **Indonesia –** Law requires that the provider of an electronic system must make upmost effort to protect personal data and immediately report any failures to law enforcement or the supervising regulatory authority of the relevant sector.
- **South Korea –** PIPA (Personal Information Protection Act) requires the Data Handler to notify affected subjects without delay of the details, circumstances and the remedial steps planned.
- **India –** The Government has established and authorised the Indian Computer Emergency Response Team (Cert-In), to collect, analyse and disseminate information on cyber incidents, provide forecast and alerts of cyber security incidents, provide emergency measures for handling cyber security incidents and coordinate cyber incident response activities.

New concepts and key principles

Explicit consent

Contracts

PIAs

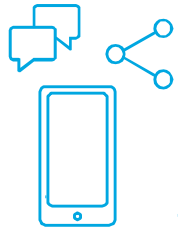


Privacy data register

Individual rights

Breach notice

Incident register



Explicit consent

Changes that will affect your organisation

European data protection law is applicable since May 2016, imposable in May 2018	Tougher sanctions for non-compliance	New data breach obligation requirements	New data privacy governance, data mapping and impact assessment requirements
Requirement to implement ‘privacy by design and default’	Strengthening of individuals’ rights to personal data	Increased focus on accountability	Data processors will have obligations too
Consent requirements will change	Data protection officers may need to be assigned	Requirements for transferring data outside the EEA	Information requirements

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 – 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 – 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.

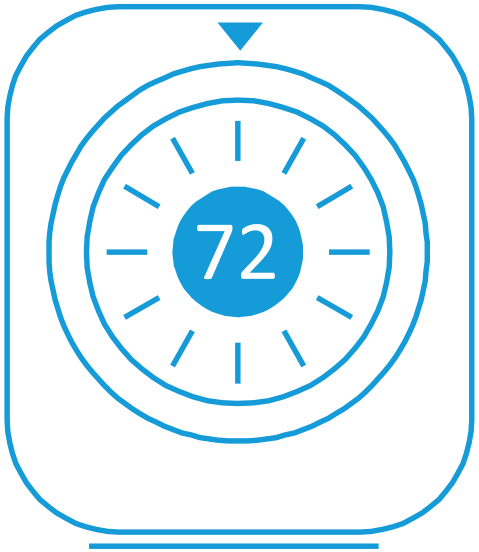
Key Changes – individual rights

Right to request that businesses delete 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

Not an absolute right - organisations may continue to process where there is legitimate grounds for it to continue e.g. compliance with a legal obligation, freedom of expression, public interest

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

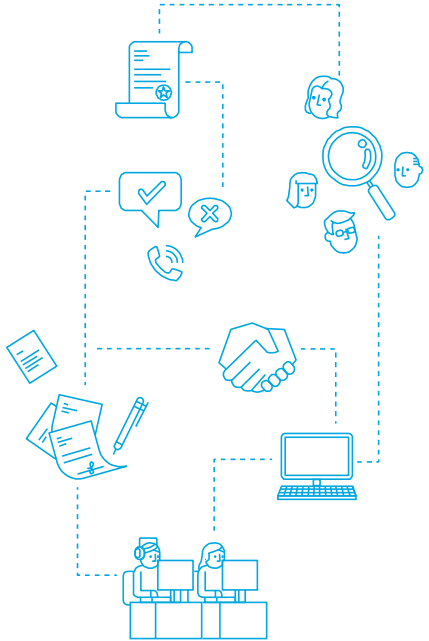
If organisations do not comply, they face a maximum fine of:

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

Key activities we are seeing (1)

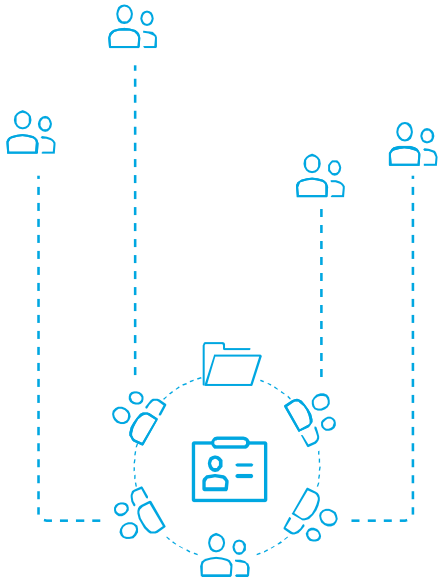
Carry out an information audit and data flow mapping exercise

Update all policies and procedures to reflect changes

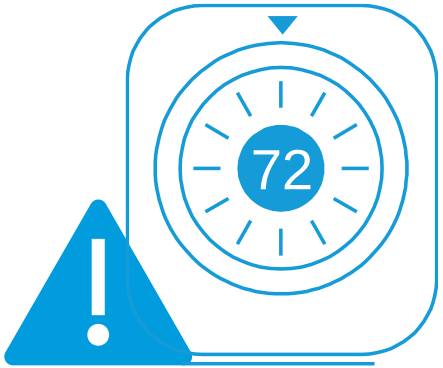


Reviewing data-related service provider contracts to reflect impact of the GDPR on controller and processor obligations

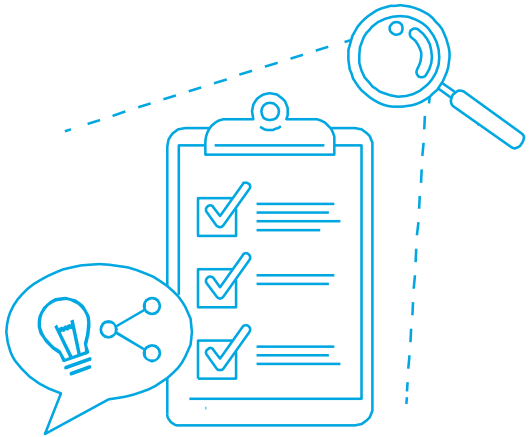
Key activities we are seeing (2)



Form a data governance group

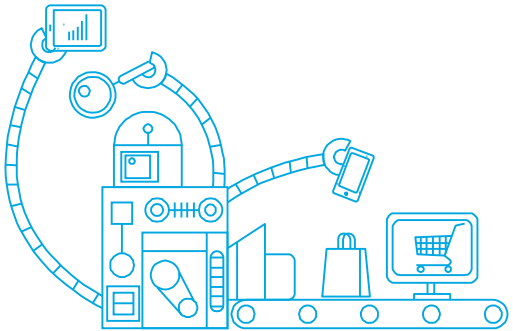


Implement / review breach notification procedures and Incident Management Plans

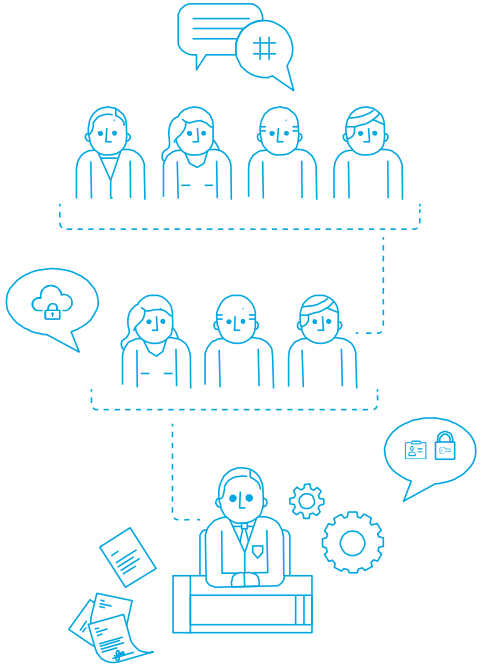


Review impact of GDPR on data retention policies e.g. on archiving

Key activities we are seeing (3)



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

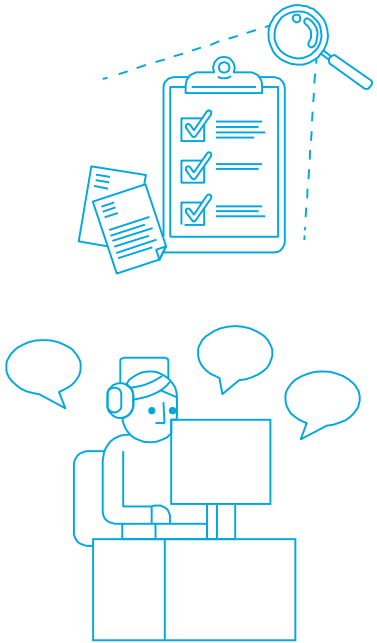


Consider the position of the existing DPO within the management structure

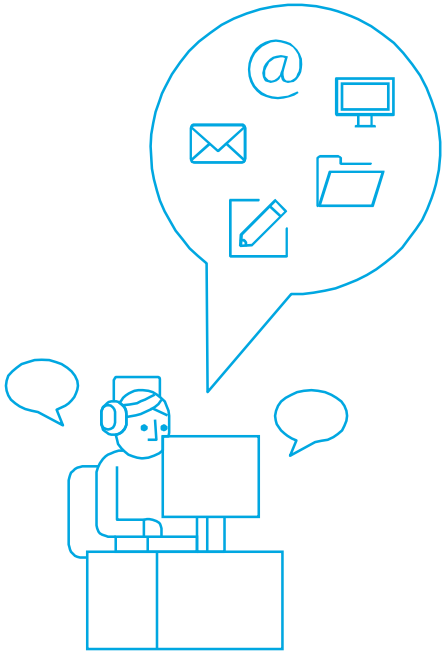
Consider and record lawful bases for processing

Key activities we are seeing (4)

Create and maintain an information asset register



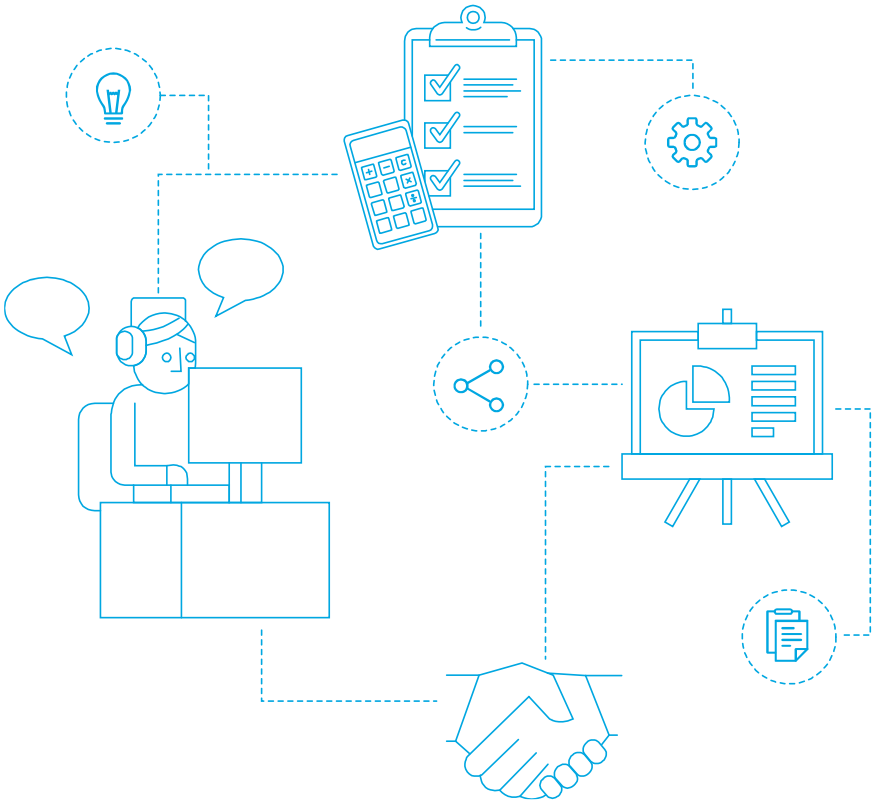
Check accountability for data governance is clear and precise



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

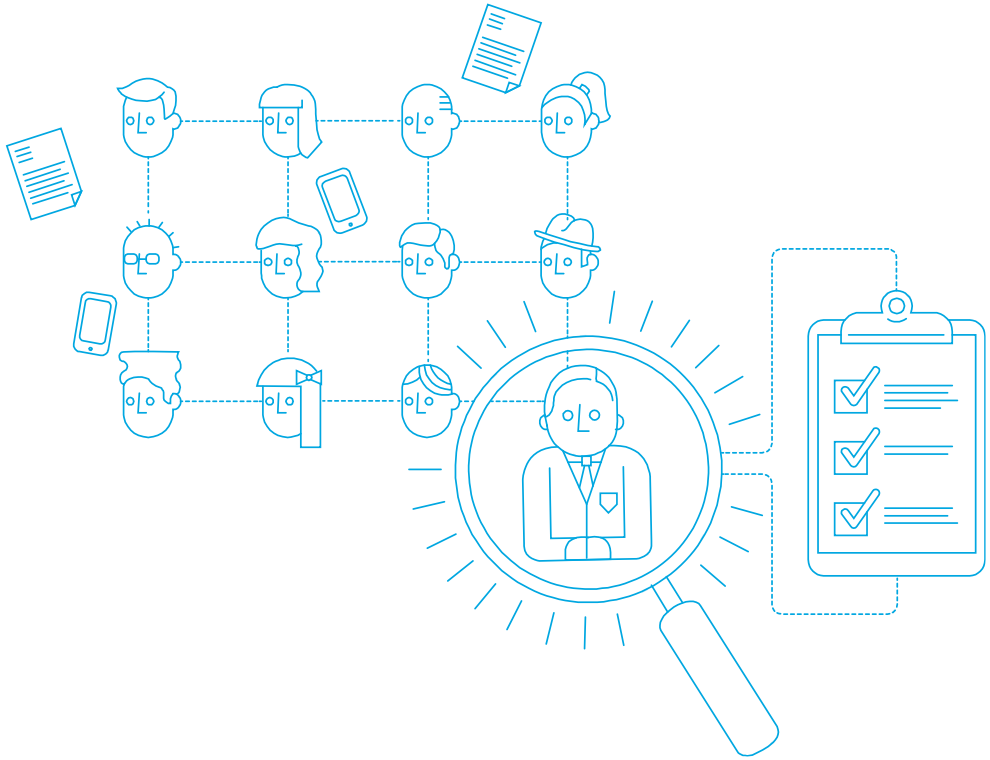
GDPR ROADMAP TO COMPLIANCE

Mobilisation



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

Discovery

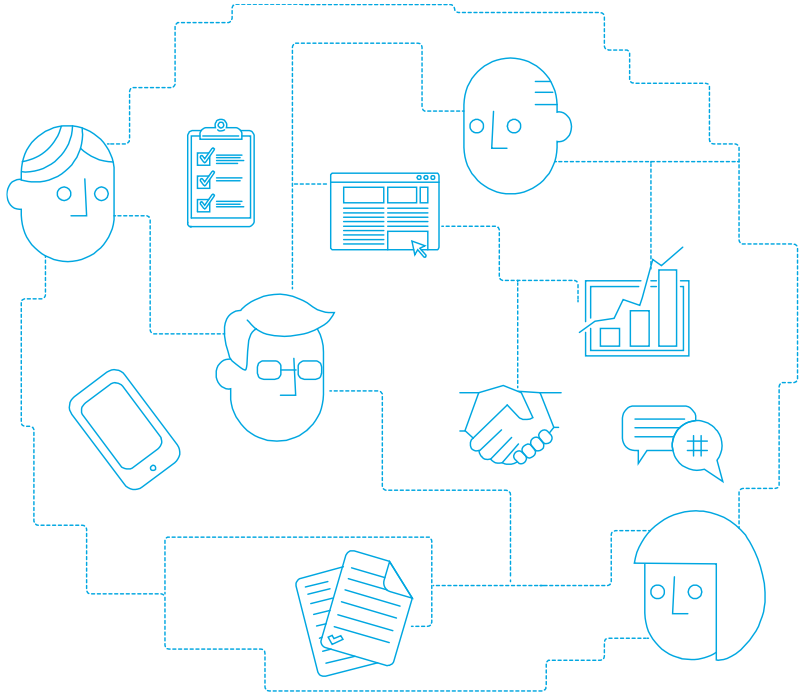


- Review documentation
- Interviews
- Review policies & procedures
- Discuss functionality of systems to meet the GDPR requirements

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

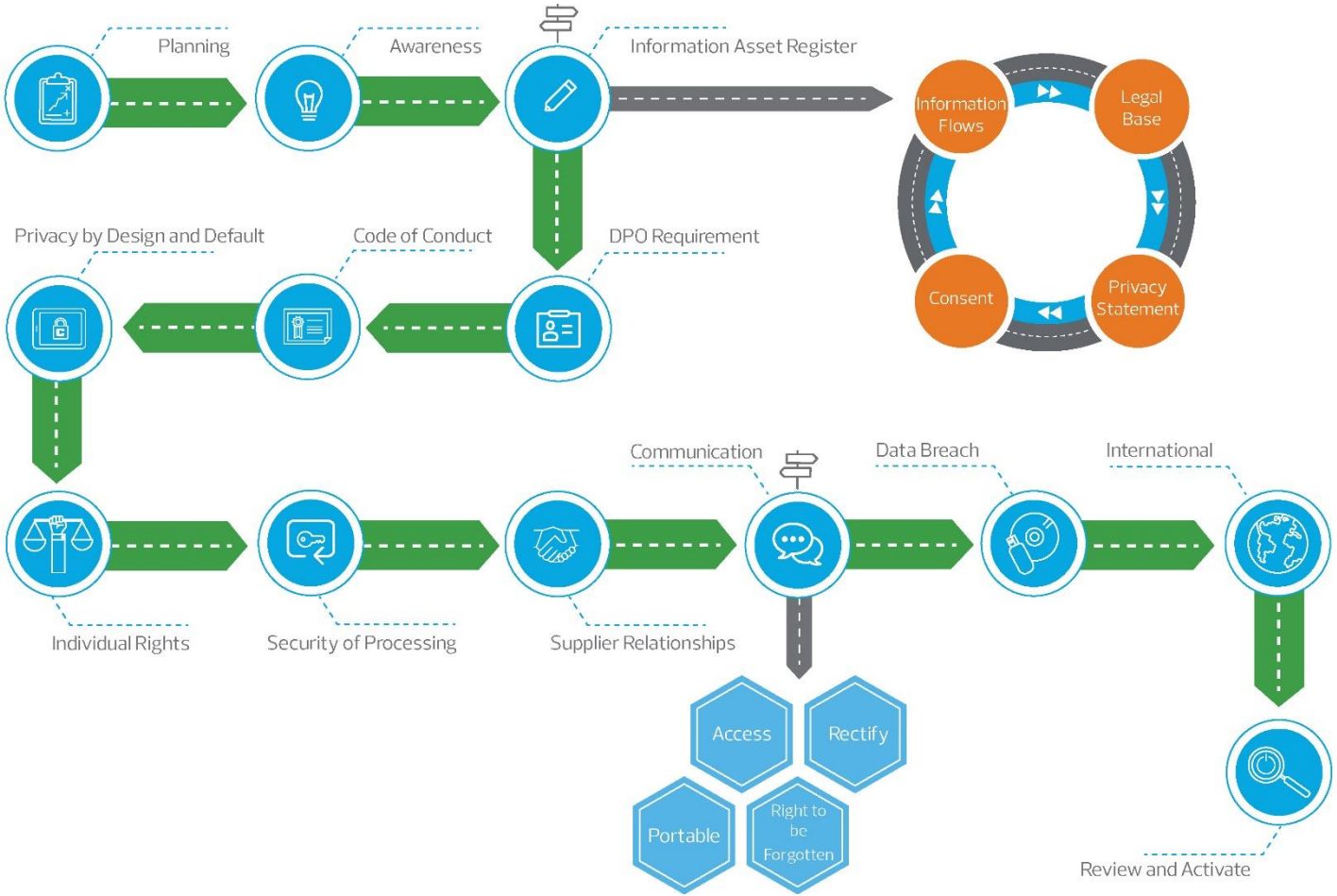
Reporting



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

GDPR

ROADMAP TO COMPLIANCE

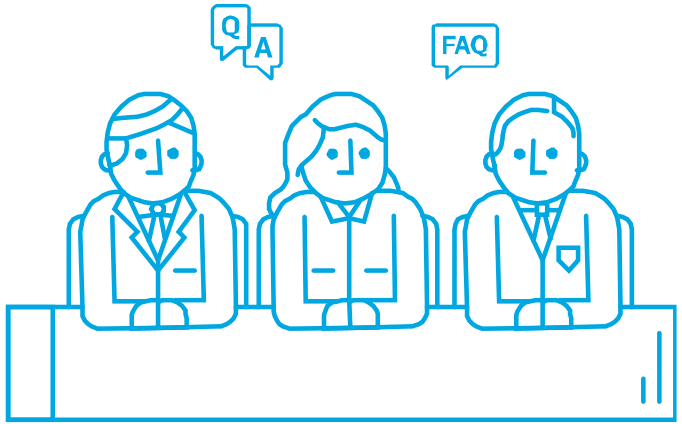


Finally

REMEMBER:

You have until 25 May 2018 to become GDPR compliant

If you have any questions or would like help with getting ready for GDPR, please contact lauren.summers@rsm.global who will put you in touch with a GDPR expert in RSM.



Thank you for your time and attention.