Deloitte.

Data Protection & Privacy Services Catalogue

Cyber Risk

MAKING AN
IMPACT THAT
MATTERS
since 1845

We take a collaborative approach to help our clients navigate new challenges and ideas.

"

We have built on our existing service offerings through the recently developed Privacy Catalogue to support organisations in transforming their privacy programme from a piecemeal approach to one that is both robust and sustainable.

Deloitte takes a holistic view toward achieving and maintaining privacy compliance. Our portfolio and capabilities range from advising organisations on their policies, strategies and operating models, training and awareness campaigns, all the way up to handling delicate and technical breach response activities.

Our service offerings form the backbone of a successful privacy transformation. Our privacy experts identify compliance and operational gaps and tailor our advisory services to the specific needs of our clients.
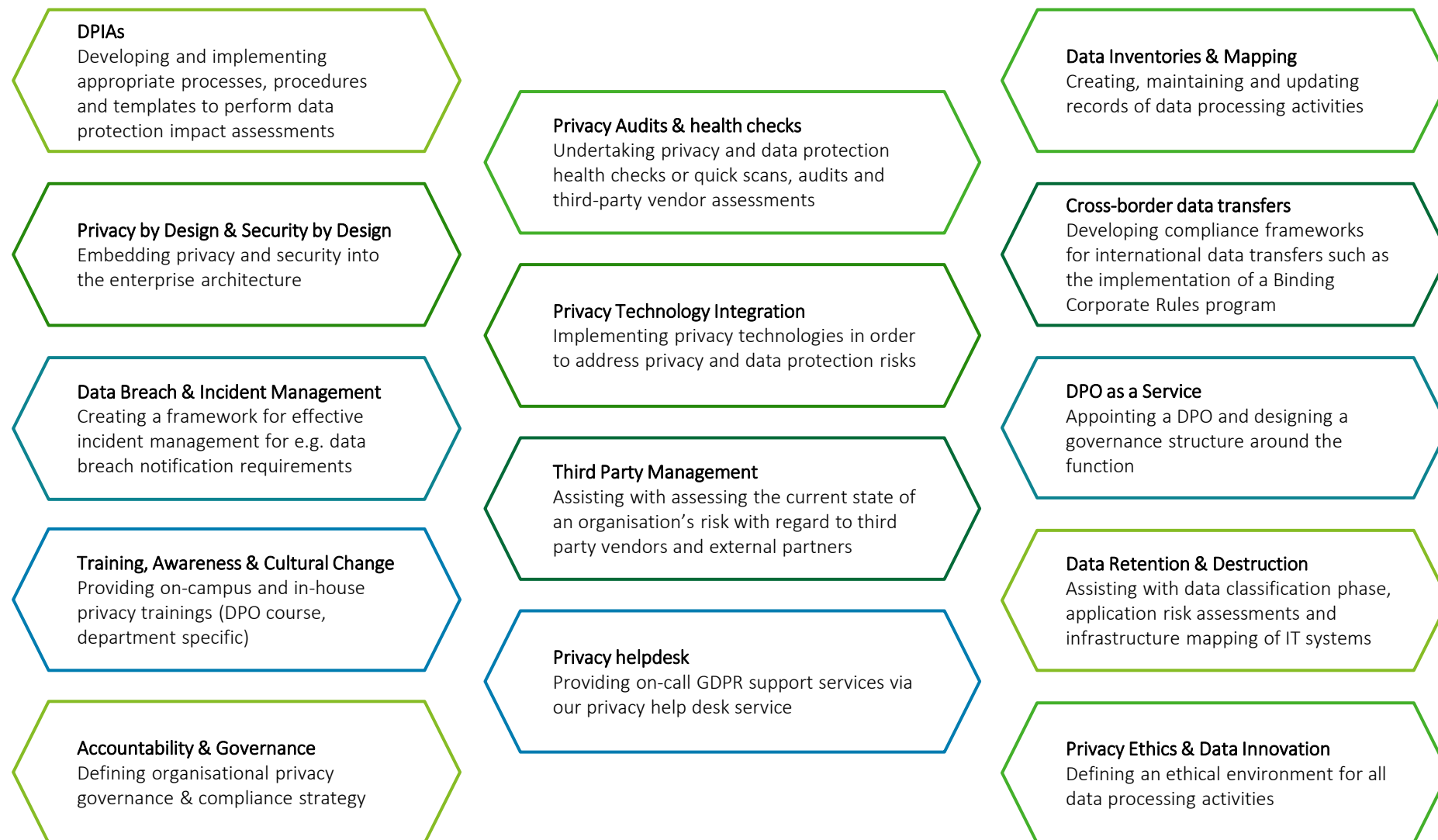
"

Data protection & privacy services catalogue

Overview of our services

DPIAs
Developing and implementing appropriate processes, procedures and templates to perform data protection impact assessments

Privacy by Design & Security by Design
Embedding privacy and security into the enterprise architecture

Data Breach & Incident Management
Creating a framework for effective incident management for e.g. data breach notification requirements

Training, Awareness & Cultural Change
Providing on-campus and in-house privacy trainings (DPO course, department specific)

Accountability & Governance
Defining organisational privacy governance & compliance strategy

Privacy Audits & health checks
Undertaking privacy and data protection health checks or quick scans, audits and third-party vendor assessments

Privacy Technology Integration
Implementing privacy technologies in order to address privacy and data protection risks

Third Party Management
Assisting with assessing the current state of an organisation's risk with regard to third party vendors and external partners

Privacy helpdesk
Providing on-call GDPR support services via our privacy help desk service

Data Inventories & Mapping
Creating, maintaining and updating records of data processing activities

Cross-border data transfers
Developing compliance frameworks for international data transfers such as the implementation of a Binding Corporate Rules program

DPO as a Service
Appointing a DPO and designing a governance structure around the function

Data Retention & Destruction
Assisting with data classification phase, application risk assessments and infrastructure mapping of IT systems

Privacy Ethics & Data Innovation
Defining an ethical environment for all data processing activities

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Data protection & privacy services catalogue
DPIAs

This service is focused on developing and implementing appropriate processes, procedures and templates to perform data protection impact assessments (DPIAs).

Main activities

- Define a risk methodology to define when a processing activity is to be considered "high risk" and should be subject to a DPIA
- Define a DPIA methodology, procedure and reporting template
- Assess the risk the processing activity brings for the rights and freedoms of the affected individuals
- Identify appropriate measures to mitigate the risks identified during a DPIA
- Define relevant data protection and security system requirements based on GDPR requirements (e.g. erasure, data export capabilities)

Key deliverables

- Risk methodology
- DPIA methodology, procedure and report template
- DPIA report
- Data protection and security requirements for systems, applications and tools processing personal data

The ADDED VALUE of a DPIA
Why should you conduct a DPIA for data processing activities carried out by your organisation?

- "Think Privacy" mentality in the organisation
- Operationalise "privacy by design"
- Promote data subject trust and confidence
- Identify and fix privacy problems at an early stage
- Meet regulatory requirements and accountability obligations
- Connect security and privacy best practice
- Achieve full functionality of processing activities
- Increase privacy and data protection awareness

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Data protection & privacy services catalogue
Data inventories & mapping

This service is focused on creating, maintaining and updating records of your organisation's processing activities (ROPAs) as per the requirements of, for example, article 30 of GDPR. In addition, we explore the possibilities of visualising your personal data flows through the use of data flow maps.

Main activities

- Create, maintain and update a centralised inventory of processing activities
- Develop a process for regularly updating the inventory of processing activities and to keep track of the changes by implementing an audit trail
- Develop a process to classify personal data (while leveraging any existing data classification policies)
- Visualise the records of processing activities in order to picture personal data flows from entry to exit point within the organisation

Deliverables

- Inventory of processing activities
- Process to classify personal data
- Process to create, maintain and update inventory of processing activities
- Data flow maps
- Procedure to develop, maintain and update data flow maps

Controller/Processor	Purpose	Data subjects
Name and contact details of the controller/Processor (entity owner of this Record of Processing Activities)	Handle intake of applications for employee candidates	Applicants

Data types	Recipients	Transfers
CV, name, home/work telephone number, email address, home address…	Recruitment agency	France, USA

Cross-border adequacy measures (Yes/No) - explain	Retention period	Security Measures
Binding Corporate Rules	1 year	MFA
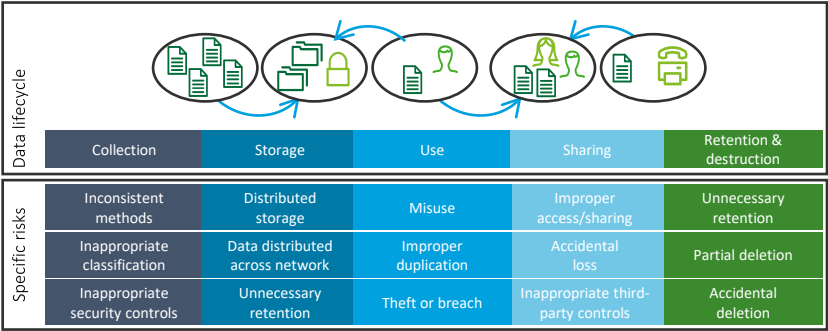
Data lifecycle				
Collection	Storage	Use	Sharing	Retention & destruction

Specific risks				
Inconsistent methods	Distributed storage	Misuse	Improper access/sharing	Unnecessary retention
Inappropriate classification	Data distributed across network	Improper duplication	Accidental loss	Partial deletion
Inappropriate security controls	Unnecessary retention	Theft or breach	Inappropriate third-party controls	Accidental deletion

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Data protection & privacy services catalogue
Data protection & security by design

This service is focused on identifying appropriate measures to embed and incorporate data protection principles and security concepts into new business and technology initiatives.
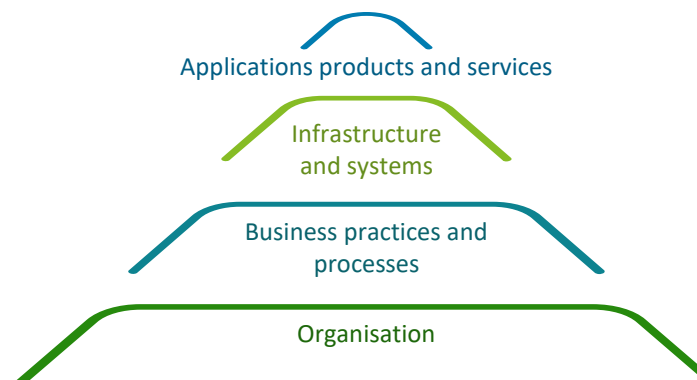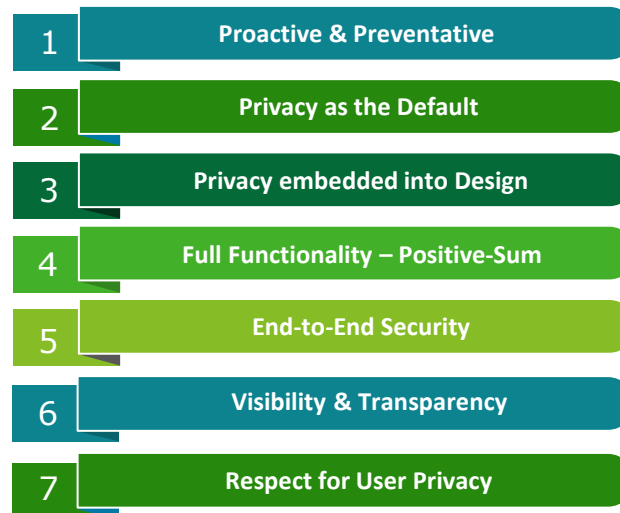
Main activities

- Develop an internal process to identify the client's high-risk business processes and corresponding systems
- Identify the "trigger" processes through which new data protection and security issues can be captured and the Data Protection & Security by Design process can be started
- Define a Data Protection & Security by Design procedure and draft process to have the principles of data protection by design and by default for identified processes and applications
- Use safety-aware programming standards

Key deliverables

- Data protection & security by design and by default process
- Data protection & security by design and by default best practices
- Workflow for new processes and systems design to meet requirements of data protection & security by design and by default principles

1 Proactive & Preventative
2 Privacy as the Default
3 Privacy embedded into Design
4 Full Functionality – Positive-Sum
5 End-to-End Security
6 Visibility & Transparency
7 Respect for User Privacy

Applications products and services

Infrastructure and systems

Business practices and processes

Organisation

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Data protection & privacy services catalogue
Cross-border data transfers

This service is focused on the inventory of your cross-border data transfers outside of the European Economic Area (EEA) in order to identify and take appropriate measures for the protection of personal data that are transferred to third countries.

Main activities

- Map out international data transfers to third countries outside of the EEA
- Identify and analyse the inherent risk level associated with each data transfer
- Identify appropriate mitigating measures to ensure that cross-border data transfers outside of the EEA are covered by appropriate safeguards in line with the provisions of the GDPR
- Adjust contracts, standard contractual clauses and binding corporate rules where necessary

Key deliverables

- Inventory of cross-border data transfers outside of the EEA
- Risk scoring methodology for cross-border data transfers
- Overview of mitigating measures to reduce risk level associated with an international data transfer

1 Scoping Questions

- E.g. What is the data processing activity?
- E.g. What types of personal data are being processed?
- E.g. Where is it transferred to?
- E.g. Which safeguarding mechanism are you using?

2 Risk Assessment

- **Low** – e.g. Adequacy Decision
- **Medium** – e.g. Standard Contractual Clauses, Binding Corporate Rules, Derogations, etc.
- **High** – e.g. Privacy Shield

3 Mitigation Actions

- Recommendations to follow
- Measures to implement

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Data protection & privacy services catalogue
Data breach and incident management

This service is focused to build a data breach and incident management procedure in alignment with identified regulatory, contractual, and policy requirements.
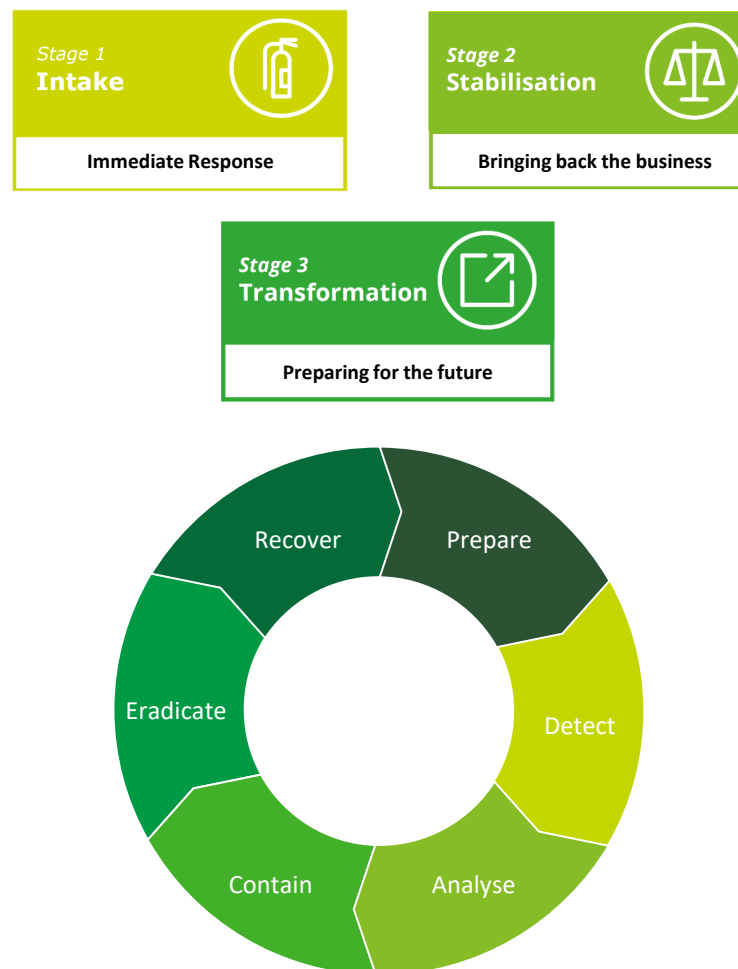
Main activities

- Draft the data breach and incident identification and notification process aligned to applicable data protection law
- Develop workflows to identify, analyse and respond to personal data breaches and to notify it to the supervisory authorities and data subjects
- Develop a process and templates for third parties to report personal data breaches and incidents without undue delay
- Draft templates to perform the root-cause-analysis of the personal data breach and to report the documentation regarding a data breach to senior management

Key deliverables

- Data breach and incident identification and notification process
- Workflows to identify, analyse, respond and report personal data breaches
- Process for third parties to report data breaches
- Templates for reporting data breaches internally and externally

Stage 1
Intake

Immediate Response

Stage 2
Stabilisation

Bringing back the business

Stage 3
Transformation

Preparing for the future

Recover — Prepare — Detect — Analyse — Contain — Eradicate

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Data protection & privacy services catalogue
Training, awareness & cultural change

This service is focused on ensuring that employees are aware of their responsibilities regarding personal data protection.
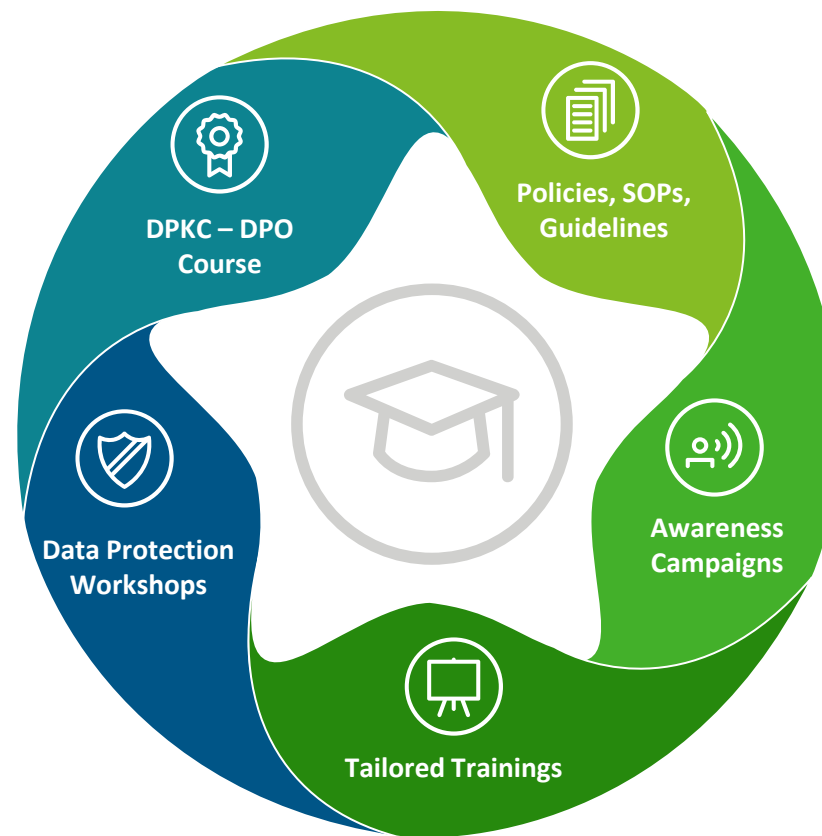
📖 Main activities

- Draft a data protection policy which sets out employees' responsibilities and refers to specific procedures such as DPIAs, Data Protection by Design, complaint handling, data breaches and so on
- Draft guidelines with do's and don'ts for specific scenarios such as data subject requests, data breaches and so on
- Design a data protection training program including the following aspects: the type of training to be given to employees, mode of training (ex-cathedra, information sessions, and so on), and mapping each training module to a business unit (or other stakeholder group)
- Organise data protection training sessions and workshops
- Design a privacy awareness campaign

📑 Key deliverables

- Awareness-raising activities
- Data protection trainings for staff involved in data processing operations
- Brochures
- Policies, Standard Operating Procedures (SOP's), Guidelines
- General data protection trainings, exercises, final assessment and certificates
- Tailored trainings with materials, exercises, final assessment and certificates

DPKC – DPO Course

Policies, SOPs, Guidelines

Data Protection Workshops

Awareness Campaigns

Tailored Trainings

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Data protection & privacy services catalogue

Accountability & governance

This service is focused organisational accountability in order to enable you to enhance trust, create new business opportunities, and insert privacy into your organisations' DNA.

📖 Main activities

- Assure the ongoing effectiveness of technical and organisational measures with regular audits and compliance assessments
- Assess the performance and improvement of the accountability framework on a continuous basis
- Define a top-down strategy involving all levels of the organisation with clear roles and responsibilities
- Draft a privacy program, processes, control plan and metrics, to ensure continuous monitoring and demonstrate accountability

Key deliverables

- Implementation of the Privacy Information Management System (PIMS) aligned with ISO/IEC 27701
- Implementation of a tailored privacy program
- Implementation of controls and metrics to monitor privacy compliance
- Implementation of a Roadmap for privacy implementation in your organisation

Privacy Governance (cycle):
- Strategy
- Governance structure and documentation
- Enterprise privacy policy
- Privacy program SOPs
- Training and awareness
- Metrics and reporting
- Program maintenance

Accountability (hexagons):
- Certifications
- Leadership and Governance
- Risk Management
- Technical and Organisational Measures
- Audit and Compliance
- Monitoring and Improvement

- Overview of our services
- **Our services catalogue**
- Our approach
- Why Deloitte?

Data protection & privacy services catalogue
Privacy audits & health checks

This service is focused on the assessment of your organisation's privacy protection policies and procedures in light of current laws and regulatory requirements.

Main activities

- Audit the organisation's privacy and security practices in order to provide a rating score per data protection domain
- Define which areas of the organisation's privacy program need to be remediated and with which level of priority
- Identification, assessment and mitigation of privacy and security risks in all relevant processes and functions throughout the organisation

Key deliverables

- Audit Reports
- Remediation plan
- Privacy Maturity and GAP Assessment Report

Heatmap Summary	Risk Level Description	Requirements & Priorities	Requirements for Providers
Critical Risks	Critical, the event will lead to a serious incident.	Critical, to be undertaken immediately	Must be eliminated
Important Risks	Important, the event should lead to a significant incident.	Important, to be undertaken quickly	Must be eliminated unless risk reduction is impossible and subject to acceptance
Moderated Risks	Moderate, the event could lead to a broad incident.	Moderate, to be undertaken at a later stage	Must be disposed of or made acceptable through appropriate control and subject to acceptance
Acceptable Risks	Acceptable, the event would lead to a significant, but isolated, internal anomaly.	Acceptable, to be continuously monitored	Acceptable without conditions
Negligible Risks	Negligible, the event would only lead to an insignificant anomaly.	Negligible, to be monitored later	Negligible

- Overview of our services
- **Our services catalogue**
- Our approach
- Why Deloitte?

Data protection & privacy services catalogue
Privacy technology integration

This service is focused on the identification and implementation of privacy management tools in order to address privacy and data protection risks through automation.
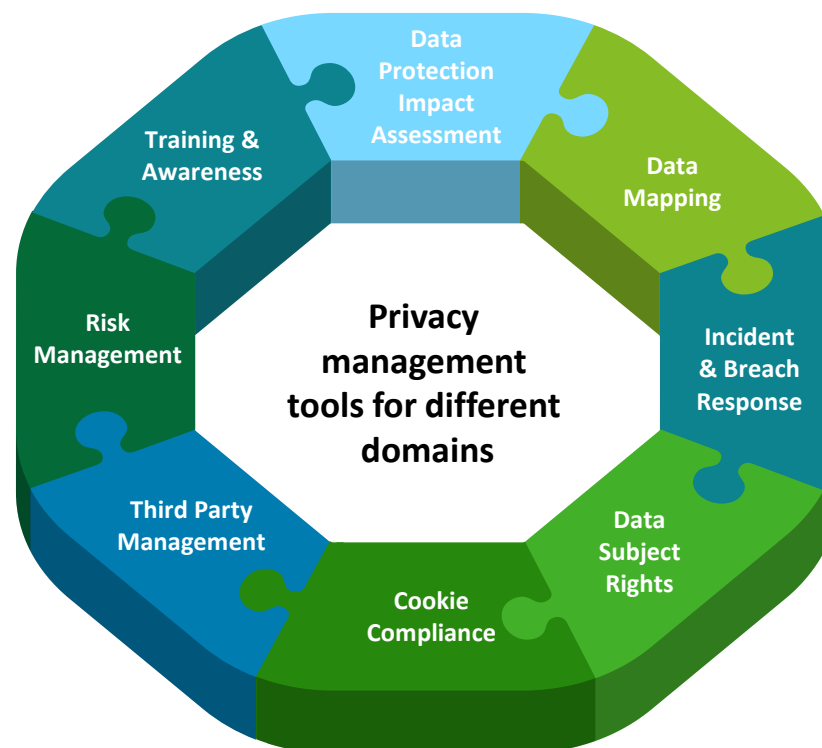
Main activities

- Identify **data protection domains** where technology can be leveraged to improve the overall maturity of the privacy program (e.g. consent management, assessment automation, third party management, cookie compliance etc.)
- Compare available tools on the market against each other in order to support you to select the most suitable technology for your organisation
- Assist and support the implementation of technology in collaboration with your internal key stakeholders, based on our understanding of your privacy program and the need for deployment of technology in certain data protection areas
- Define privacy operating models, process flows, roles and responsibilities and develop support guidelines for all profiles included in the models

Key deliverables

- Overview of data protection domains where technology can support to improve the overall maturity of the privacy program
- Support the implementation of privacy management tools (e.g. OneTrust, Collibra, BigID…) to improve the maturity of your privacy program
- Support the creation of guidelines and materials on how to use the implemented privacy management tools
- Support the post-implementation management of the tool implemented in your organisation on a daily basis

Privacy management tools for different domains

- Data Protection Impact Assessment
- Data Mapping
- Incident & Breach Response
- Data Subject Rights
- Cookie Compliance
- Third Party Management
- Risk Management
- Training & Awareness

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Data protection & privacy services catalogue
Third party management

This service is focused on the management of interactions with external parties with which your organisation has a contractual relationship.
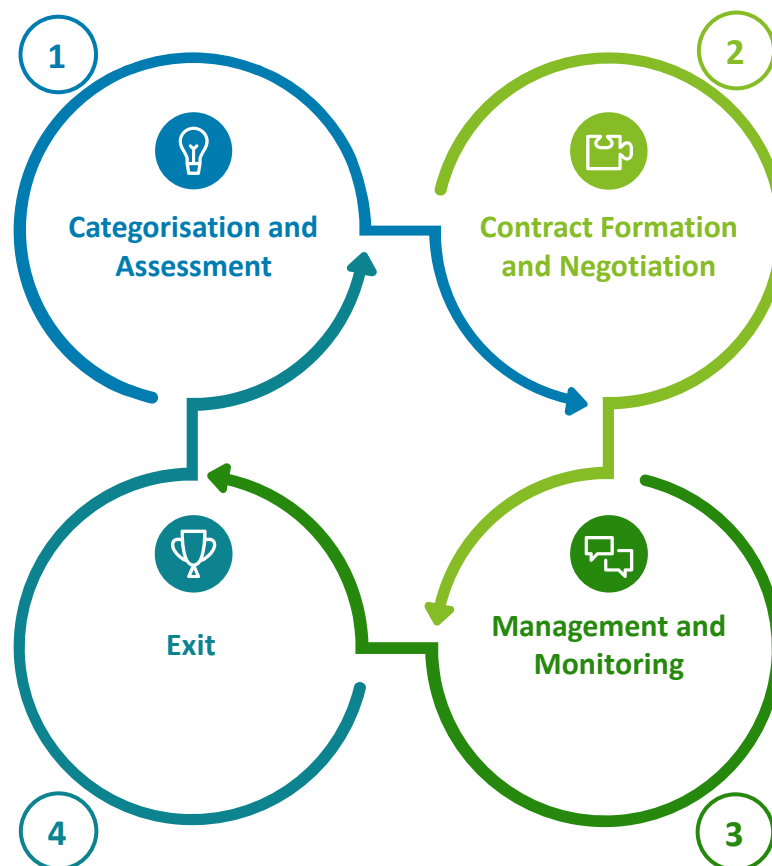
Main activities

- Update the centralised inventory of processing activities (if required) in order to include the categories of third parties with whom the organisation shares personal data
- Develop, maintain and update the third-party register in order to identify third party processors who process personal data on behalf of the organisation. Enable audit trail in order to keep track of any changes to the register
- Establish a third-party contract database, which includes all contracts with third-party processors and corresponding data processing agreements
- Develop a risk ranking methodology in order to score third party processors based on their data processing practices
- Establish a methodology to evaluate third-party relationships in order to take the necessary measures to comply with EU data protection requirements for international data transfers and in line with recent developments under the Schrems II judgement

Key deliverables

- Enhanced third party register
- Reviewed third party contract database
- Third party risk scoring methodology
- Due-diligence questionnaire and self-assessment checklist for third parties
- Third party and sub-processor contract best practices
- Procedure for off-boarding a third party

1 Categorisation and Assessment

2 Contract Formation and Negotiation

3 Management and Monitoring

4 Exit

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Data protection & privacy services catalogue
DPO as a service

This service is focused on the appointment, function and position of the DPO within your organisation and on the design of a data protection governance structure, as well as the interface with other relevant stakeholders.

📖 Main activities

- Determine and document the need to appoint a DPO (under GDPR) and document the decision taken
- Draft a clear and complete DPO job description, which includes the mandatory tasks of the DPO
- Provide advice on the recommended position, reporting line and staffing of the DPO function
- Define recommended interaction points of the DPO with other relevant functions (e.g. IT, marketing, HR, data governance)

Key deliverables

Key deliverables highly dependent on the particular nature of the service and needs of the organization:

- Legal advice regarding the appointment of a DPO
- Data protection governance structure

DPO as a service

- Information and Advice
- Training and Awareness Campaigns
- Data Breach Management and Supervisory Authorities
- Monitoring
- Increase Security Level
- Data Protection by Design and by Default

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Data protection & privacy services catalogue
Privacy helpdesk

This service is focused on offering a flexible privacy helpdesk to relevant stakeholders responsible for data protection within your organisation such as the data protection officer (DPO).
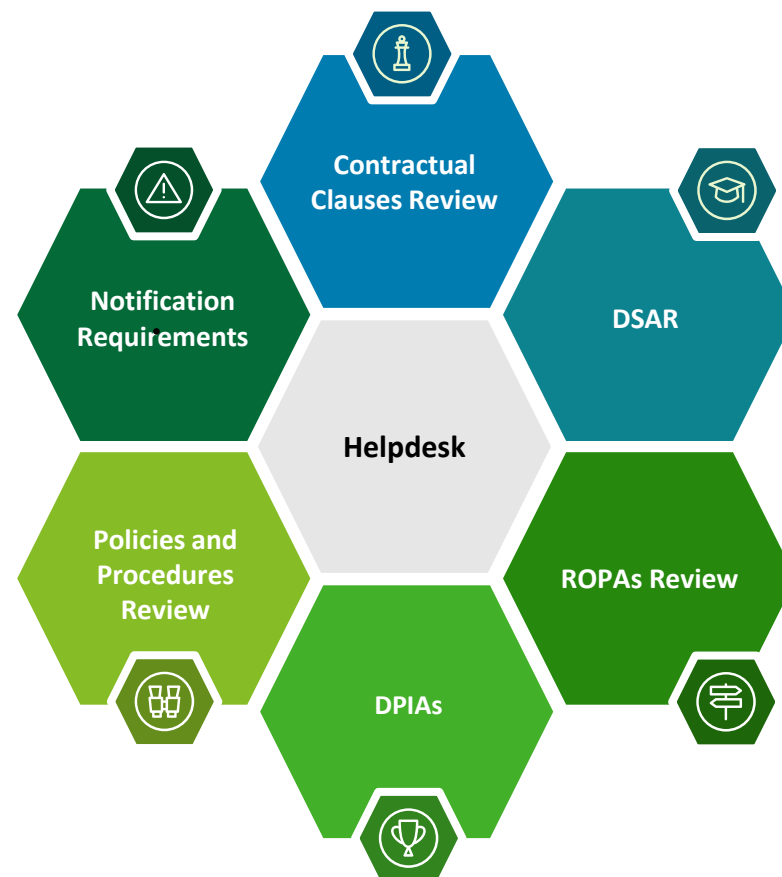
Main activities

- Provide ad-hoc advice to relevant internal stakeholders, such as the DPO, regarding any legal or practical question you may have regarding the interpretation and implementation of the requirements of applicable data protection law
- Perform ad-hoc activities such as the review of privacy policies and procedures, review of records of processing activities, support the performance of data protection impact assessments (DPIA), etc

Key deliverables

Key deliverables highly dependent on the particular nature of the service and needs of the organization:

- Ad-hoc privacy advice as flexible support to the DPO
- Ad-hoc activities such as review of policies and procedures, performance of a DPIA etc

Contractual Clauses Review

Notification Requirements

DSAR

Helpdesk

Policies and Procedures Review

ROPAs Review

DPIAs

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Data protection & privacy services catalogue
Data retention & destruction

This service is focused on defining data retention periods for different types of personal data based on legal obligations and business needs; and identifying adequate measures to ensure personal data is properly deleted.

Main activities

- Define appropriate data retention periods for different types of personal data, considering the legal obligations applicable to the company (based on legal research) as well as the company's business needs (based on previously obtained knowledge of business)
- Validate data retention periods with the relevant business teams and obtain sign-off from relevant stakeholders
- Document data retention periods into a data retention policy which lists the maximum retention period for each relevant type of personal data
- Identifying adequate technical measures to ensure data retention periods are effectively implemented
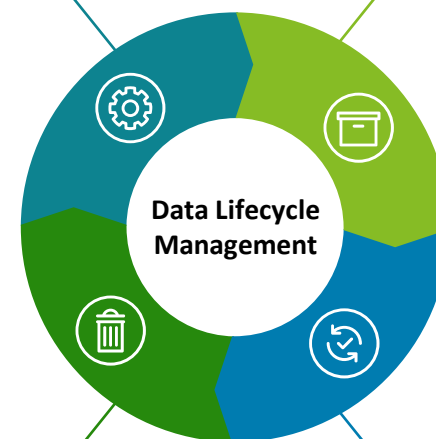
Key deliverables

- Draft data retention and destruction policies and procedures
- Creation of training and communication related to data retention and destruction
- Organisational and technical measures to ensure data disposal and erasure (e.g. best practice advice regarding e-mail management)

Creation

Storage/Usage

Data Lifecycle Management

Destruction

Retention

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Data protection & privacy services catalogue
Privacy ethics and data innovation

This service is focused on the ability for your organisation to process personal data in a transparent an ethical environment.
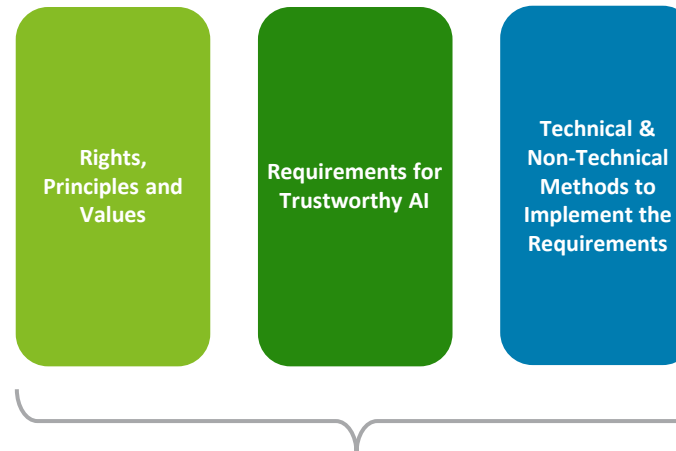
Main activities

- Ensure that all envisaged personal data processing activities are clearly defined and assessed
- Establish, implement and maintain a data subject rights procedure, including the relevant roles and responsibilities
- Conduct a DPIA
- Strengthen Privacy and Ethics by design and by default

Key deliverables

- Draft the Privacy Policy and Privacy Statement
- Establish a roadmap and remediation plan
- Process to obtain, record and maintain consent along with audit trail
- Process to manage consent
- Process to ensure GDPR Principles and Data Subjects' Rights are adhered to
- Process to strengthen Privacy and Ethics by design and by default

Rights, Principles and Values

Requirements for Trustworthy AI

Technical & Non-Technical Methods to Implement the Requirements

Use

Analysis

Evaluation & Justification

Development

Re-design

Overview of our services
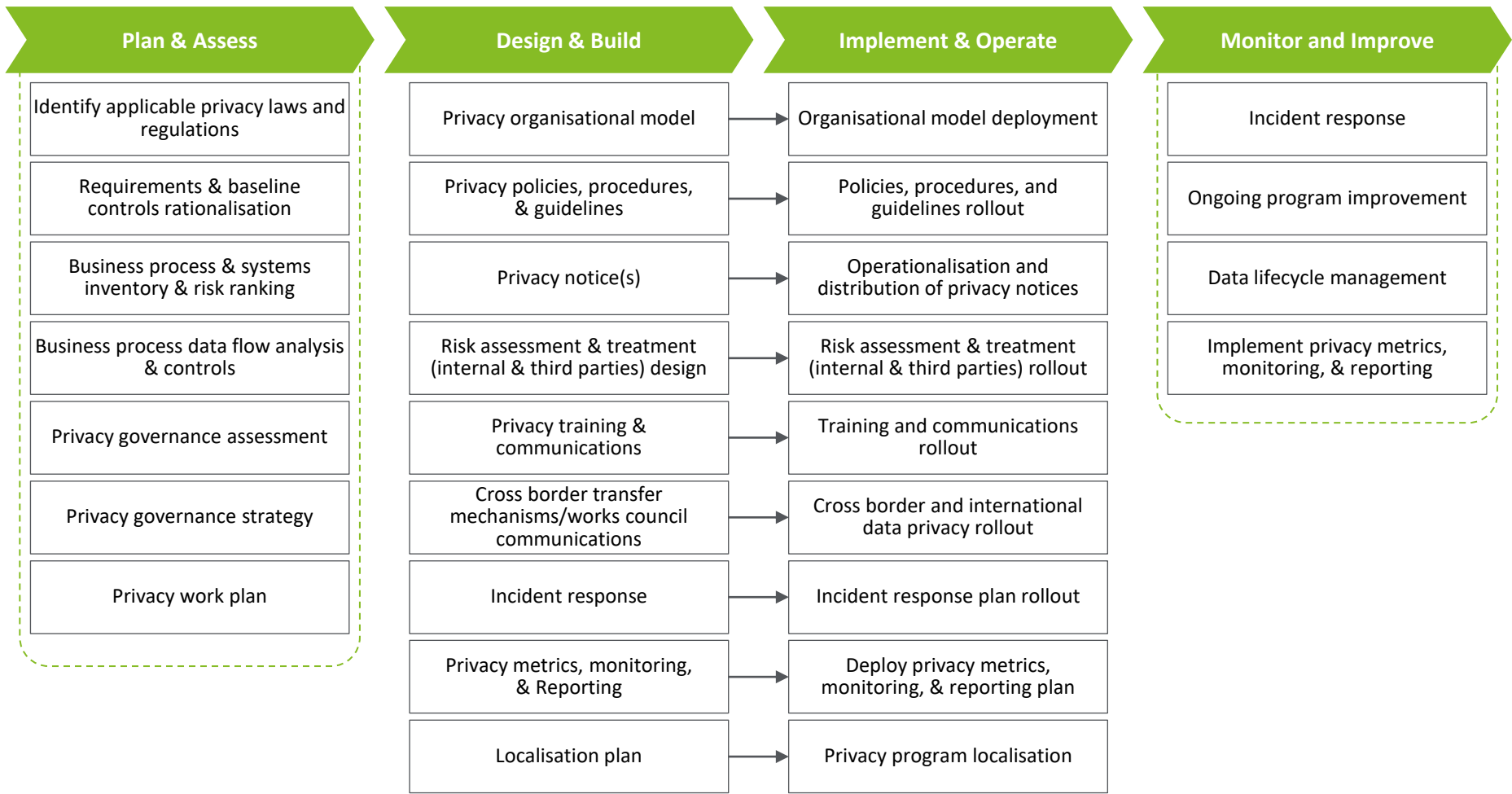
Our services catalogue

Our approach

Why Deloitte?

Our approach
Our methodological approach

Our **flexible and modularised methodology** has been utilised by numerous global organisations to build a holistic global privacy program, and includes the following key phases and activities:

Plan & Assess	Design & Build	Implement & Operate	Monitor and Improve
Identify applicable privacy laws and regulations	Privacy organisational model	Organisational model deployment	Incident response
Requirements & baseline controls rationalisation	Privacy policies, procedures, & guidelines	Policies, procedures, and guidelines rollout	Ongoing program improvement
Business process & systems inventory & risk ranking	Privacy notice(s)	Operationalisation and distribution of privacy notices	Data lifecycle management
Business process data flow analysis & controls	Risk assessment & treatment (internal & third parties) design	Risk assessment & treatment (internal & third parties) rollout	Implement privacy metrics, monitoring, & reporting
Privacy governance assessment	Privacy training & communications	Training and communications rollout	
Privacy governance strategy	Cross border transfer mechanisms/works council communications	Cross border and international data privacy rollout	
Privacy work plan	Incident response	Incident response plan rollout	
	Privacy metrics, monitoring, & Reporting	Deploy privacy metrics, monitoring, & reporting plan	
	Localisation plan	Privacy program localisation	

Overview of our services

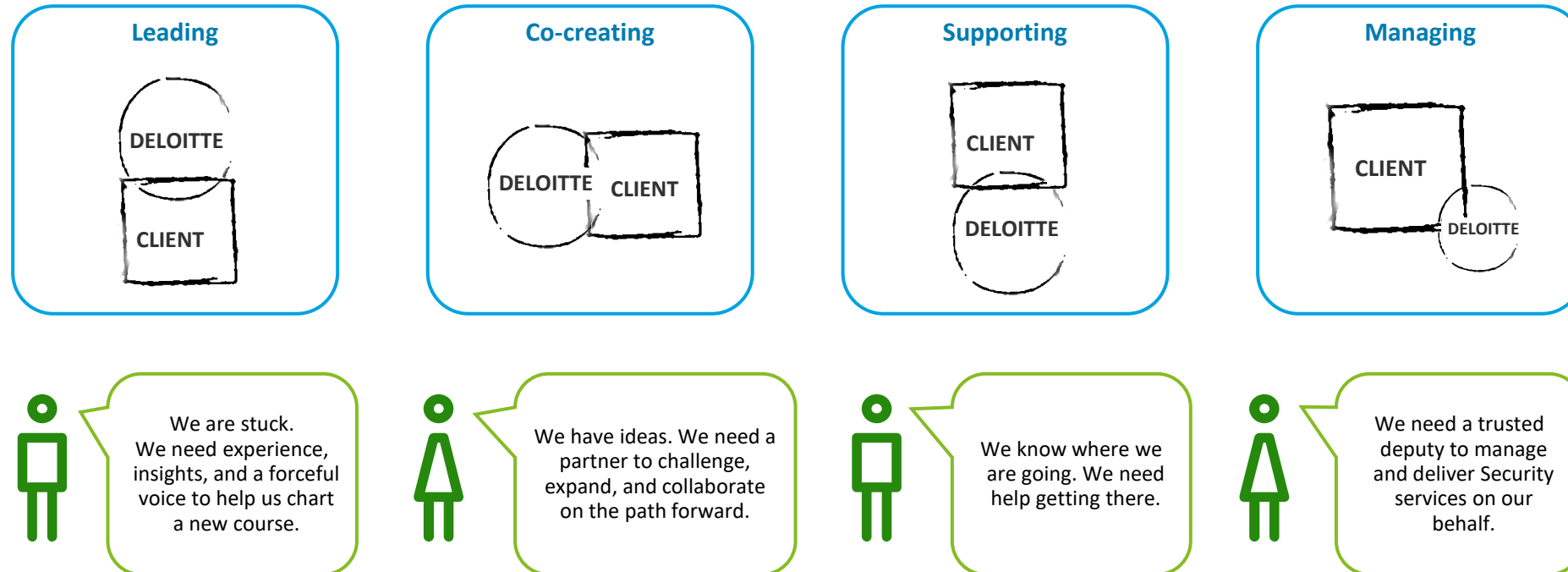Our services catalogue

Our approach

Why Deloitte?

Our approach
How we interact with out clients

There are times when our clients need a forceful voice. Other times they need a partner. Once in a while, they need a consultant to support them on the journey or a deputy to manage security services on their behalf. And there are times when they need all four — maybe even on the same initiative.

For some consultants, that kind of flexibility is uncomfortable. At Deloitte, we embrace these clients' needs. The only thing that matters to us: **to deliver the expected results to our clients, the way they need them delivered at the exact moment.**

Leading	Co-creating	Supporting	Managing
DELOITTE / CLIENT	DELOITTE / CLIENT	CLIENT / DELOITTE	CLIENT / DELOITTE

We are stuck. We need experience, insights, and a forceful voice to help us chart a new course.

We have ideas. We need a partner to challenge, expand, and collaborate on the path forward.

We know where we are going. We need help getting there.

We need a trusted deputy to manage and deliver Security services on our behalf.

We select the **optimum model** together with our client based on our initial conversations.

Overview of our services

Our services catalogue
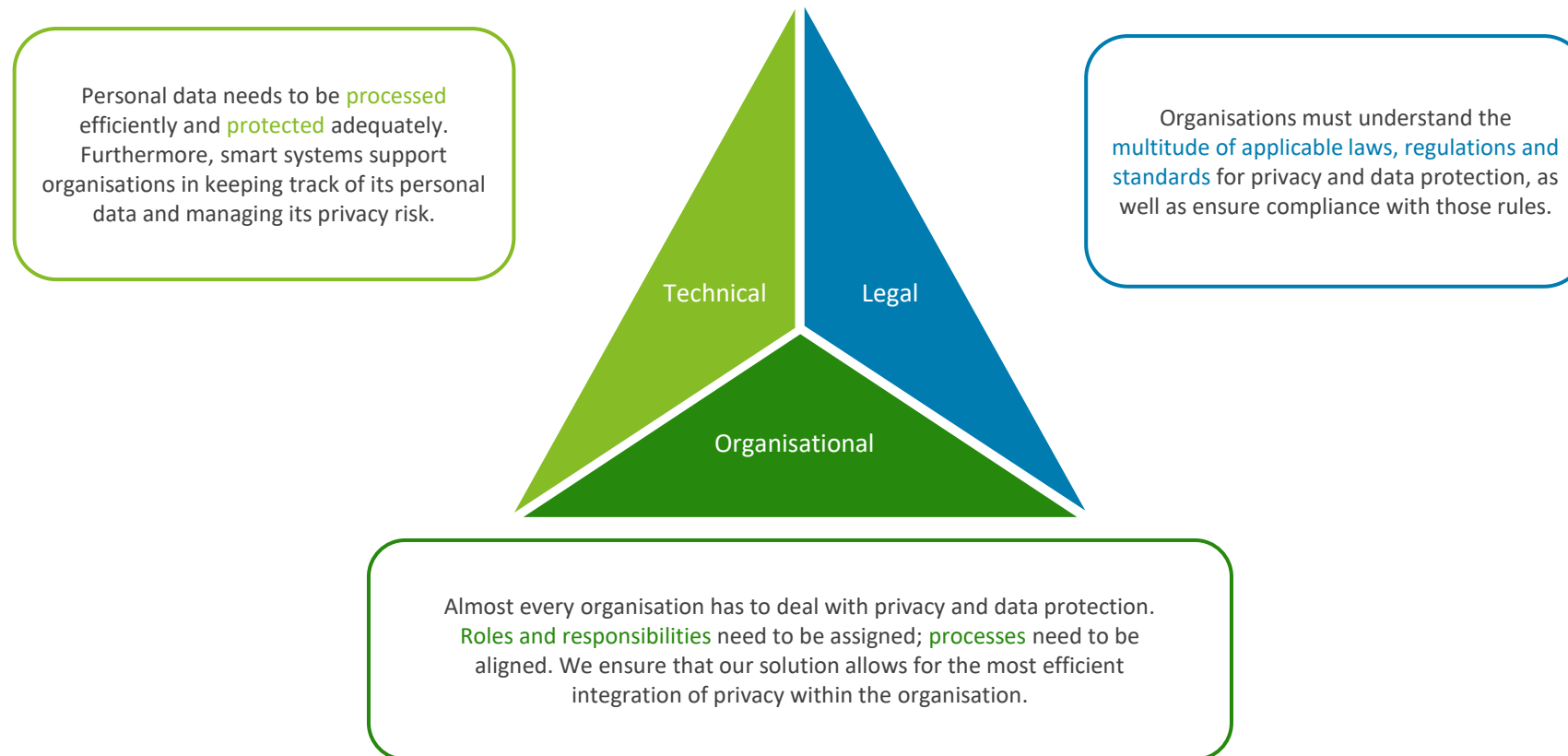
Our approach

Why Deloitte?

Why Deloitte?
A multidisciplinary effort

Privacy is a **combination** of knowledge of the law, acknowledging the enormous **technical aspects** that putting it into practice entails and the **efforts** that are required to embed this in an organisation in a manner that **fits the structure and culture.**

We strongly believe that only organisations where **privacy responsible staff** come from each of these backgrounds and are willing to learn about those two that is not their own, will succeed in running **efficient and effective privacy operations.**

We have therefore also modelled our own team accordingly: our team includes **expertise** in each of these three areas.

Personal data needs to be processed efficiently and protected adequately. Furthermore, smart systems support organisations in keeping track of its personal data and managing its privacy risk.

Organisations must understand the multitude of applicable laws, regulations and standards for privacy and data protection, as well as ensure compliance with those rules.

Technical

Legal

Organisational

Almost every organisation has to deal with privacy and data protection. Roles and responsibilities need to be assigned; processes need to be aligned. We ensure that our solution allows for the most efficient integration of privacy within the organisation.

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Why Deloitte?
Our strengths

Multidisciplinary

Privacy is a combination of knowing the **law**, acknowledging the enormous **security aspects** that it entails **and the efforts that are needed to embed this in an organisation** in a way that it fits the structure and culture. We are able to advise on all these elements.

Extensive advisory experience

We use the experience from other assignments in our projects and consult with professionals that have worked on similar projects before. We use **knowledge from our experts across industries and competences**. We do this to make sure we develop efficient and effective solutions.

International focus

Our EMEA and global network includes **certified information privacy professionals and certified security professionals** bringing **dozens of years of experience** performing similar services across several jurisdictions. Through our network of member firms, we can obtain and **use local expertise** that is vital to compliance related topics.

Broad privacy experience

We are convinced that in order to deliver the best privacy advise, it is necessary to use both legal and technical and organisational expertise within the team. Our team includes not just legal expertise – we have **broad technical experience and knowledge of how privacy is best handled in large organisations**.

Leader in privacy and security

Deloitte is the largest global professional services firm and recognised leader in the privacy and security domain. We have assisted **top global banking and financial institutions** with GDPR and Privacy program readiness and implementation over the last **2 years**. **Belgium, Germany and the US** are key countries from which we have been serving global clients.

Dedicated privacy & security professionals

We are constantly supporting our clients on all instances of their **privacy journey**, by providing result-oriented expertise and strategic directions. We advise on **short-term practical solutions** but work with our clients towards **sustainability** and **economies of scale**. Our work approaches **include delivery on specific engagements**, as well **as one-stop-shop support** (Helpdesk) or combining both.

Overview of our services

Our services catalogue

Our approach

Why Deloitte?

Deloitte.

About Deloitte

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

Deloitte provides audit, tax and legal, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 312,000 professionals, all committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu

Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.