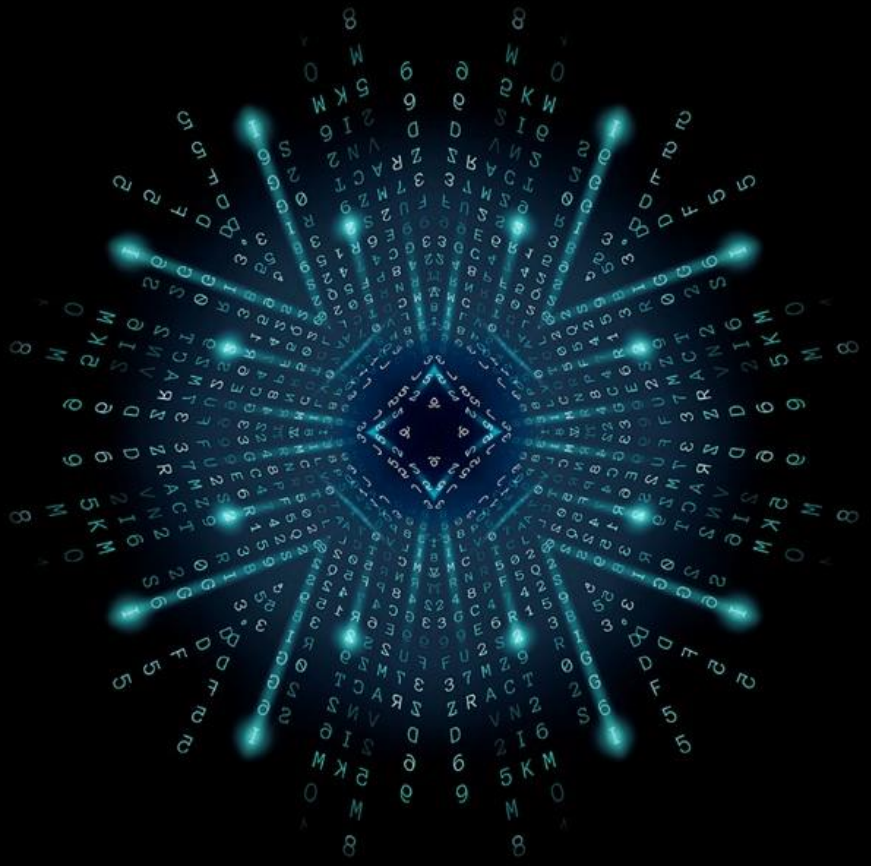
Deloitte.



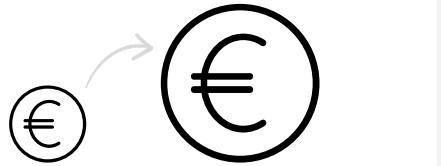
General Data Protection Regulation (GDPR)

Deloitte NWE Privacy Services – Vision and Approach

Deloitte Risk Advisory - 2018

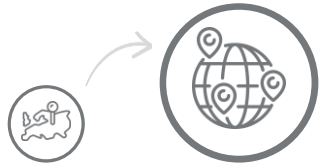
The Big Picture

Key elements of the GDPR



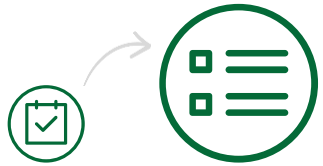
FINES UP TO 4% OF GLOBAL TURNOVER

Previously fines were limited in size and impact. GDPR fines will apply to both controllers and processors.



INCREASED TERRITORIAL SCOPE

GDPR will apply to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location.



EXPLICIT AND RETRACTABLE CONSENT

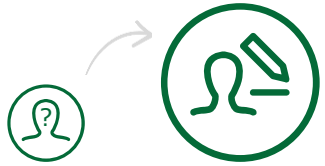
Must be provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

DATA SUBJECT RIGHTS

Data subjects can request confirmation whether or not their personal data is being processed, where and for what purpose. Additionally, data subjects can request to be forgotten, which entails the removal of all the data related to the data subject.

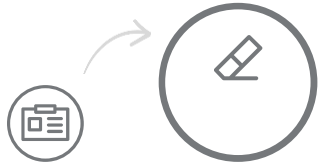
BREACH NOTIFICATION WITHIN 72 HOURS

Security breaches involving personal data may need to be reported to the authorities within 72 hours after detection and possibly be reported to individuals as well.



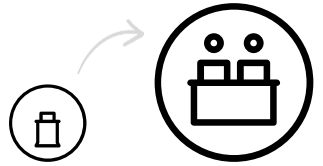
PRIVACY BY DESIGN

Now a legal requirement for the inclusion of data protection from the onset of the designing of systems, rather than a retrospective addition.



DATA INVENTORY

Organizations must maintain a record of processing activities under its responsibility – or, in short, they must keep an inventory of all personal data processed. The inventory must include the multiple types of information, such as the purpose of the processing.



MANDATORY DATA PROTECTION OFFICERS

Appointed in certain cases to facilitate the need to demonstrate compliance to the GDPR and to compensate for no longer requiring bureaucratic submission of data processing activities or transfers based on Model Contract Clauses.

Deloitte Vision on GDPR

Organisational impact

The GDPR impacts many areas of an organisation: legal and compliance, technology, and data

Legal and Compliance

The GPDR introduces new requirements and challenges for legal and compliance functions. Many organisations will require a Data Protection Officer (DPO) who will have a key role in ensuring compliance. It is estimated that 28,000 new DPOs will be required in Europe alone. If the GDPR is not complied with, organisations will face the heaviest fines yet – up to 4% of global turnover. A renewed emphasis on organisational accountability will demands proactive, robust privacy governance, requiring organisations to review how they write privacy policies, to make these easier to understand.

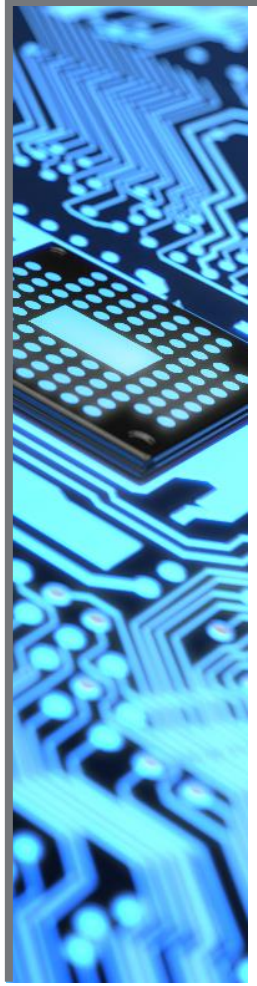
Chief Risk Officer

Privacy Officer

Chief Compliance Officer

General Counsel

Technology



New GDPR requirements will mean changes to the ways in which technologies are designed and managed. Documented privacy risk assessments will be required to deploy major new systems and technologies. Security breaches will have to be notified to regulators within 72 hours, meaning implementation of new or enhanced incident response procedures. The concept of 'Privacy By Design' has now become enshrined in law, with the Privacy Impact Assessment expected to become commonplace across organisations over the next few years. And organisations will be expected to look more into data masking, pseudonymisation and encryption.

Chief Information Officer

Chief Information Security Officer

Data

Individuals and teams tasked with information management will be challenged to provide clearer oversight on data storage, journeys, and lineage. Having a better grasp of what data is collected and where it is stored will make it easier to comply with (new) data subject rights – rights to have data deleted and to have it ported to other organisations.

Chief Data Officer

Chief Operating Officer

Vision – Legal and Compliance

General Counsels, Chief Compliance Officers, Chief Privacy Officers and Data Protection Officers: Your privacy strategies, resourcing, and organisational controls will need to be revised. Boardrooms will need to be engaged more than ever before.

1 A Revolution in Enforcement

Fines of up to 4% of annual global turnover

Serious non-compliance could result in fines of up to 4% of annual global turnover, or €20 million – whichever is higher. Enforcement action will extend to countries outside of the EU, where analysis on EU citizens is performed. But how will this play out in practice? Will US organisations, for example, take heed of EU data protection authorities?

2 Accountability

Proactive approach

The current requirement to provide annual notifications of processing activities to local regulators will be replaced by significant new requirements around maintenance of audit trails and data journeys. The focus is on organisations having a more proactive, comprehensive view of their data and being able to demonstrate they are compliant with the GDPR requirements.

3 Data Protection Officers

Market hots up for independent specialists

Organisations processing personal data on a large scale will now be required to appoint an independent, adequately qualified Data Protection Officer. This will present a challenge for many medium to large organisations, as individuals with sought-after skills and experience are currently in short supply.

4 Privacy Notices and Consent

Clarity and education is key

Organisations should now consider carefully how they construct their public-facing privacy policies to provide more detailed information. However, it will no longer be good enough to hide behind pages of legalese. In addition, the GDPR will retain the notion of consent as one of the conditions for lawful processing, with organisations required to obtain 'freely given, specific, informed and unambiguous' consent, while being able to demonstrate these criteria have been met.

Vision – Technology

Chief Information Officers, Chief Technology Officers and Chief Information Security Officers: Your approach towards the use of technology to enable information security and other compliance initiatives will need to be reconsidered, with costs potentially rising.

1 Breach Reporting

Breach reporting within 72 hours of detection

Significant data breaches will now have to be reported to regulators and in some circumstances also to the individuals impacted. This means organisations will have to urgently revise their incident management procedures and consider processes for regularly testing, assessing and evaluating their end to end incident management processes.

2 Online Profiling

Profiling becomes a loaded topic

Individuals will have new rights to opt out of and object to online profiling and tracking, significantly impacting direct-to-consumer businesses who rely on such techniques to better understand their customers. This applies not just to websites, but also to other digital assets, such as mobile apps, wearable devices, and emerging technologies.

3 Encryption

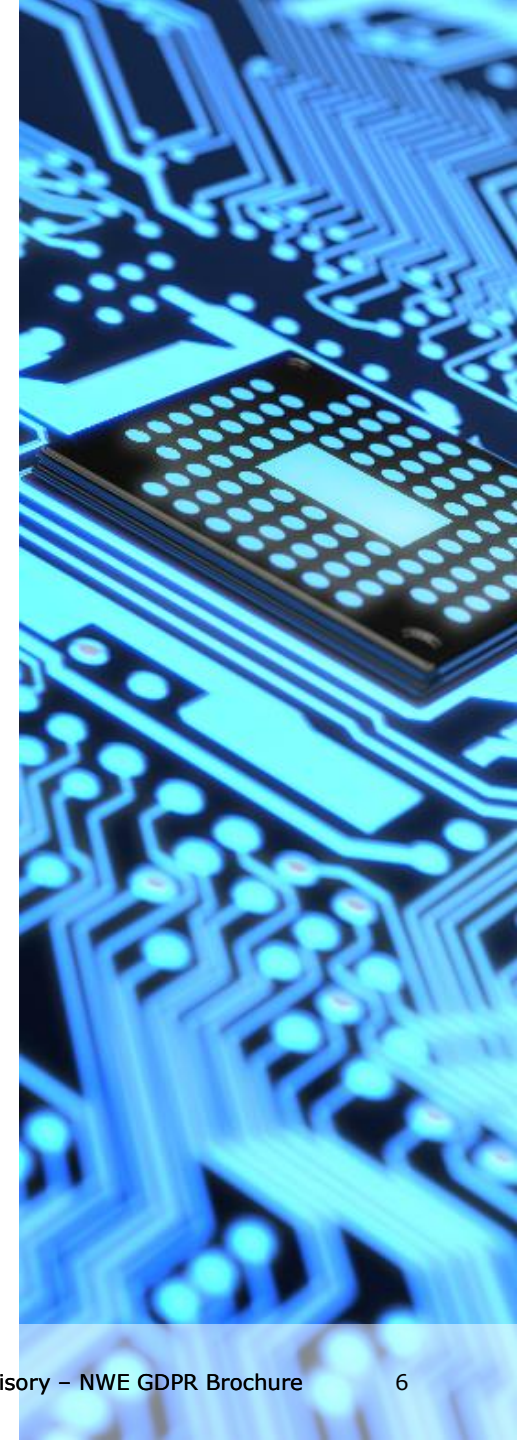
Encryption as means of providing immunity?

The GDPR formally recognises the privacy benefits of encryption, including an exemption from notifying individuals of data breaches when data is encrypted. However, this does not mean that organisations can afford to be complacent, and the exemption may not apply when weak encryption has been used. Given the potential fines, organisations will have to further increase their focus on a robust information and cyber security regime.

4 Privacy-by-Design

Recognised best practice becomes law

The concept of Privacy By Design (PbD) is nothing new, but now it is enshrined in the GDPR. Organisations need to build a mindset that has privacy at the forefront of the design, build and deployment of new technologies. The result is a design process that takes privacy (and security!) into account right from the start. In this way organisations are able to effectively and efficiently manage privacy risks when new uses of personal data are developed.



Vision – Data

Chief Data Officers, Data Stewards, Chief Marketing Officers, and Digital Leads: Your information management activities have always supported privacy initiatives, but under the GDPR new activities are required which specifically link to compliance demands.

1 Data Inventories

Identifying and tracking data

Organisations will have to take steps to demonstrate they know what data they hold, where it is stored, and who it is shared with, by creating and maintaining an inventory of data processing activities. Data leads will have to work closely with privacy colleagues to ensure all necessary bases are covered. A thorough system for maintaining inventories needs to be implemented.

2 Right to Data Portability

A new right to request standardised copies of data

A new right to 'data portability' means that individuals are entitled to request copies of their data in a readable and standardised format. The interpretation of this requirement is debatable, but taken broadly the challenges could be numerous – amongst them achieving clarity on which data needs to be provided, extracting data efficiently, and providing data in an industry-standardised form.

3 Right to be Forgotten

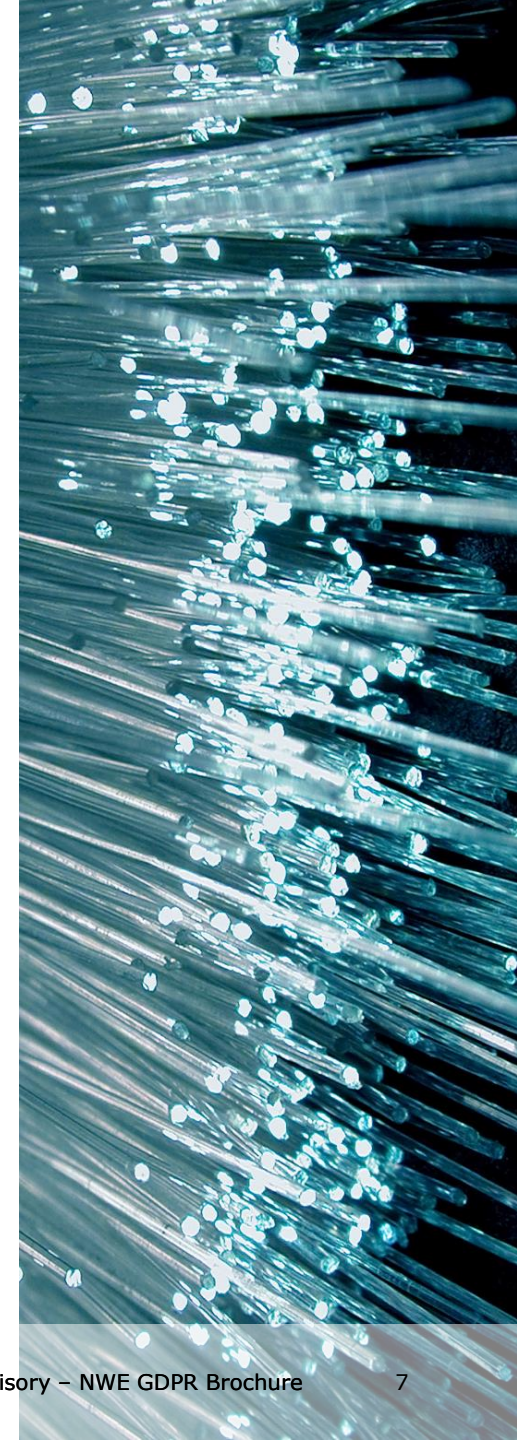
A stronger right for consumers to request deletion of their data

A new 'right to be forgotten' is further evidence of the consumer being in the driving set when it comes to use of their data. Depending on regulatory interpretation, organisations may need to perform wholesale reviews of processes, system architecture, and third party data access controls. In addition, archive media may also need to be reviewed and data deleted.

4 Definitions of Data

The concept of pseudonymisation of data

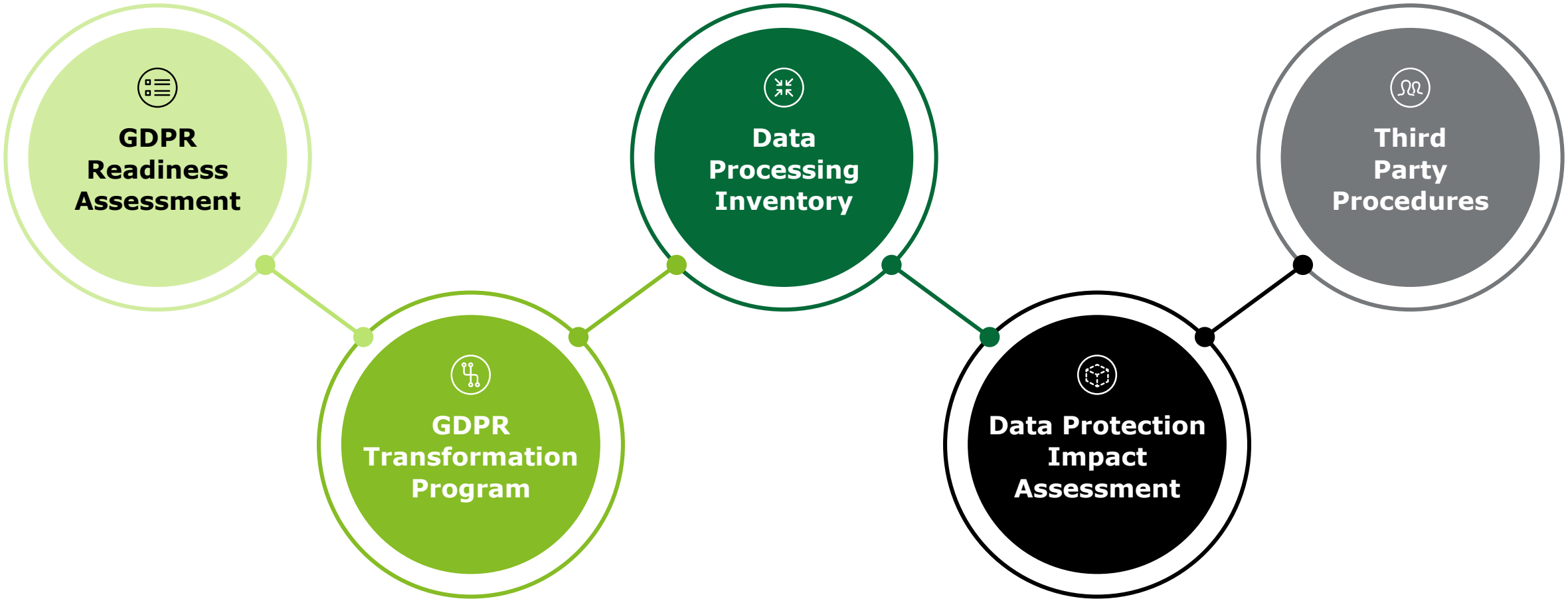
The GDPR provides for a broad definition of what data should be classified as personal data. It also expressly recognises the concept of pseudonymisation of data, while at the same time recognising that pseudonymous personal data is still subject to the GDPR's requirements. Therefore emphasis is placed on proper data classification and governance.



Deloitte Approach to GDPR

Approach – Actions to take

Actions to take to prepare for the GDPR



Approach - GDPR Readiness Assessment

The road to GDPR compliance with the GDPR Maturity Assessment & Roadmap

What is the GDPR Readiness Assessment?

To give a clear picture on where your organisation currently stands with respect to the GDPR, the GDPR Readiness Assessment is the tool of choice. The GDPR Readiness Assessment is:

- A powerful methodology, based on an existing Deloitte practice to create a baseline for privacy;
- Part of the cyber tooling suite, potential to incorporate into your broader cyber strategy and roadmap;
- Used by Deloitte globally for privacy and cyber assessments and strategy definition;
- A good starting point for becoming compliant with the GDPR and getting a tailored privacy program;
- Based on our Privacy, Security and Governance framework, covering all elements of the described privacy program;
- Instrumental in finding the areas with the biggest risk;
- Used to focus on those areas which most urgently need action to become GDPR compliant;
- A method to measure how mature the organisation currently is, using the Deloitte privacy and data protection maturity model.

First steps in becoming GDPR compliant

Our maturity approach to privacy challenges is based on industry best practices, Deloitte advisory methodology and our experience with privacy and cyber engagements at a large number of other clients. Deloitte has conducted a number of relevant benchmarks over the years, such as the Privacy Benchmark and the Governance Benchmark, which can be referenced to determine your organisation's current standing.

1

▸ Capture Business Insight

Privacy compliance & GDPR Readiness framework tailored based on industry and organisational characteristics.

2

▸ Insight in Current Privacy Situation

A thorough assessment by workshops and interviews with (a part of) the organisation, giving insight of the current level of maturity against the framework.

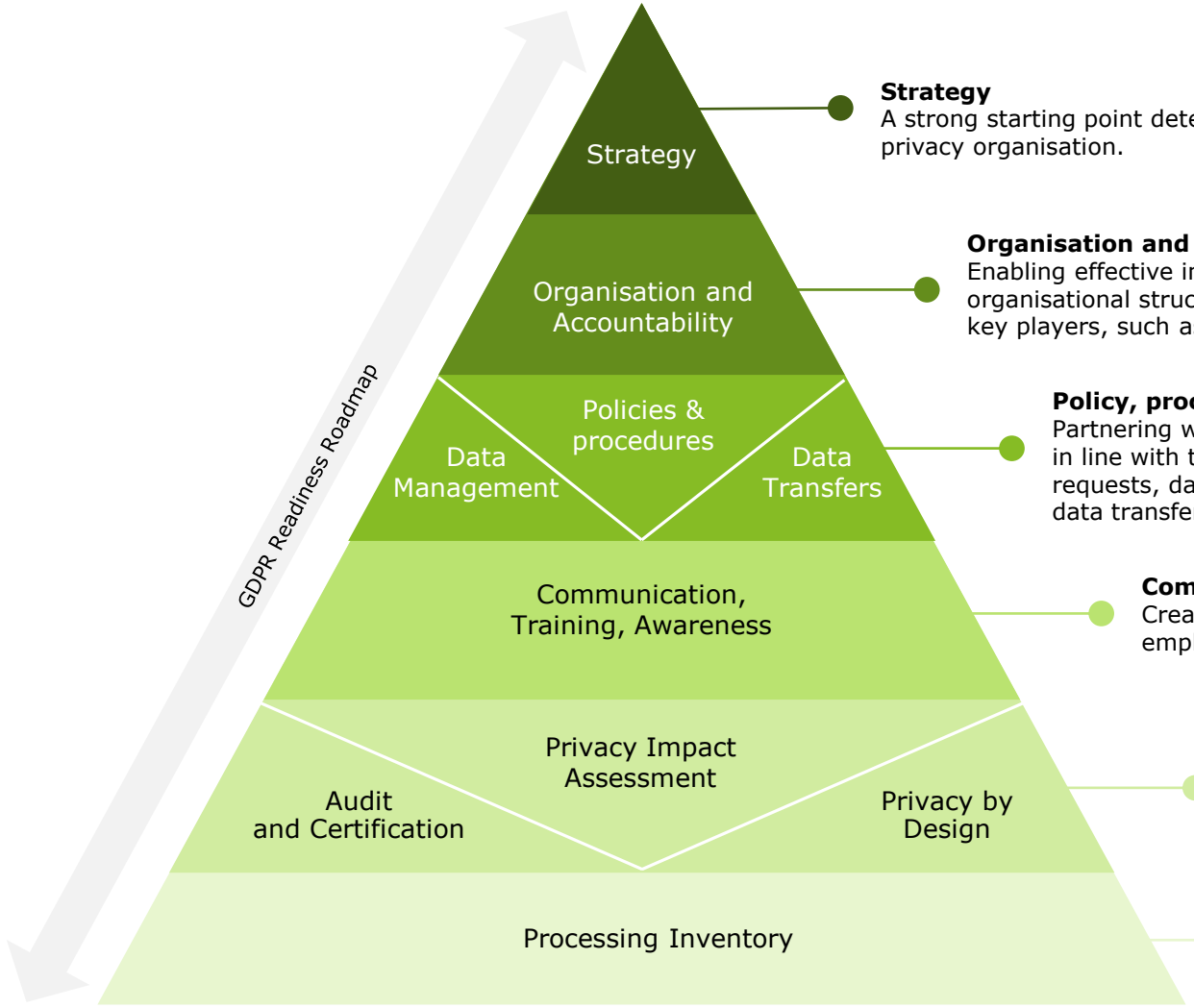
3

▸ Develop Strategy & Roadmap

A practical and concrete roadmap with prioritised steps required to improve, risk-based, the state of privacy compliance with the GDPR.

Approach - Actions to take to prepare for the GDPR

Based on a comprehensive GDPR readiness roadmap a tailored transformation program helps organisations prepare in the optimal way for the GDPR



Strategy
A strong starting point determining high level direction and risk appetite, upon which the organisation builds its privacy organisation.

Organisation and Accountability
Enabling effective implementation of the privacy strategy requires a strong and multidisciplinary privacy organisational structure. This covers the structure of the privacy organisation as well as the role and position of key players, such as the Data Protection officer. This layer also covers accountability; how to prove compliance?

Policy, process & data
Partnering with the Business to ensure data is protected, governed, managed and utilised effectively in line with the organisation's strategy. Also covers technological challenges such as data access requests, data retention, right to be forgotten, breach notification and international and 3rd party data transfers.

Communication, Training, Awareness
Creating a high level of organisational awareness on privacy ensures that the organisation's employees know and follow the rules.

Privacy Operations
Embedding privacy into the organisations project methodology. This is done by efficient and practical guidance during conception of a new or changed product or service (Privacy by Design) as well as assessing new and existing systems following the established PIA method. Also covers audit guidance and research into privacy seal certification (new option in the GDPR).

Processing Inventory
A processing inventory is a fundamental element of any privacy program, and will be a mandatory requirement following the GDPR.

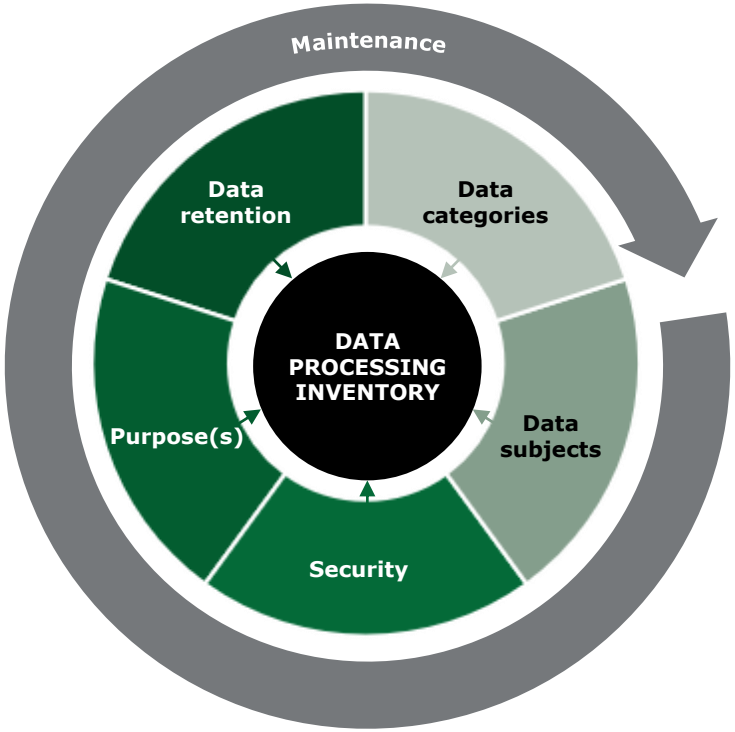
Approach - Data Processing Inventory

Creating a data inventory provides an overview of all data and insight in the risks attached to processing activities

A Data Processing Inventory is your basis to get in control of your data processing

- A data inventory is an overview which includes all the required information concerning personal data processing, such as purpose(s), categories of data and retention period.
- Having an inventory is an actual requirement under the GDPR (following from article 30), but it can also serve you well in building your understanding of the personal data you processes.
- The inventory is used as a register of all the data processes within the organisation.
- Having an inventory is essential for your oversight of processing activities and is a mandatory element of GDPR compliance.
- The inventory allows your organisation to demonstrate awareness of its obligations as a data controller, including keeping of records of processing activities.
- Finally, knowing which personal data the organisation processes mitigates the risk of unidentified data breaches.

Article 30 of the GDPR requires an up-to-date overview of processing activities



Approach – Data Protection Impact Assessments

Embedding privacy into your project methodology by assessing privacy risks in an early stage

A Tailored Approach

Privacy can be considered as an operational risk that requires practical solutions in order to make sure that risk is actually handled.

The challenge is to provide uniform and flexible methodologies and process to safeguard privacy every time a data driven project starts.

Key Elements to Consider

- Ensuring new projects and initiatives abide by the privacy rules within your organisation is done through robust Data Protection Impact Assessments (DPIAs);
- DPIAs are based on the GDPR and are a proven and effective tool to assess privacy risks;
- The **DPIA process** describes the phases of identification, DPIA and remediation covering roles, responsibilities, sign offs, escalation, support for a DPIA and should be efficient and effective;
- A **DPIA method** is the combination of checks, questions and requirements to assess the impact and risks that any system or project should follow;
- **Remediation** should always be the end phase of a DPIA and makes sure impact can be reduced and risks mitigated or accepted.

DPIA Process

Identification

- Privacy intake
- Top level risk assessment
- Prioritization

DPIA

- Legitimate grounds
- Purposes
- Maintaining internal records
- Data Quality
- Transparency
- Rights of the data subject
- Privacy by Design and by Default
- Data protection impact assessment
- Data breach notification
- Security
- Processing performed by a processor
- Transfer

Remediation

- Privacy risk assessment
- Risk mitigation
- Risk Acceptance

Approach - Third Party Procedures

External parties bring specific challenges for data controllers

Data Breach Handling Procedure

When a data breach occurs there are many internal and external challenges. Handling and communication procedures with processors, authorities and data subjects are essential for effective data breach handling.

Data Processing Agreements

Are your DPAs GDPR proof? With the new data breach rules in place there is a requirement for contractual arrangements between Controller and Processors.

Vendor Assessment

Every time your organisation uses a third party for any kind of service that might involve data processing there should be a concrete process with clear requirements to assess these parties and their specific service.

To make sure this is done effectively there needs to be collaboration between legal, risk, IT and procurement with strong steering from the DPO.

Data Subject Rights procedure

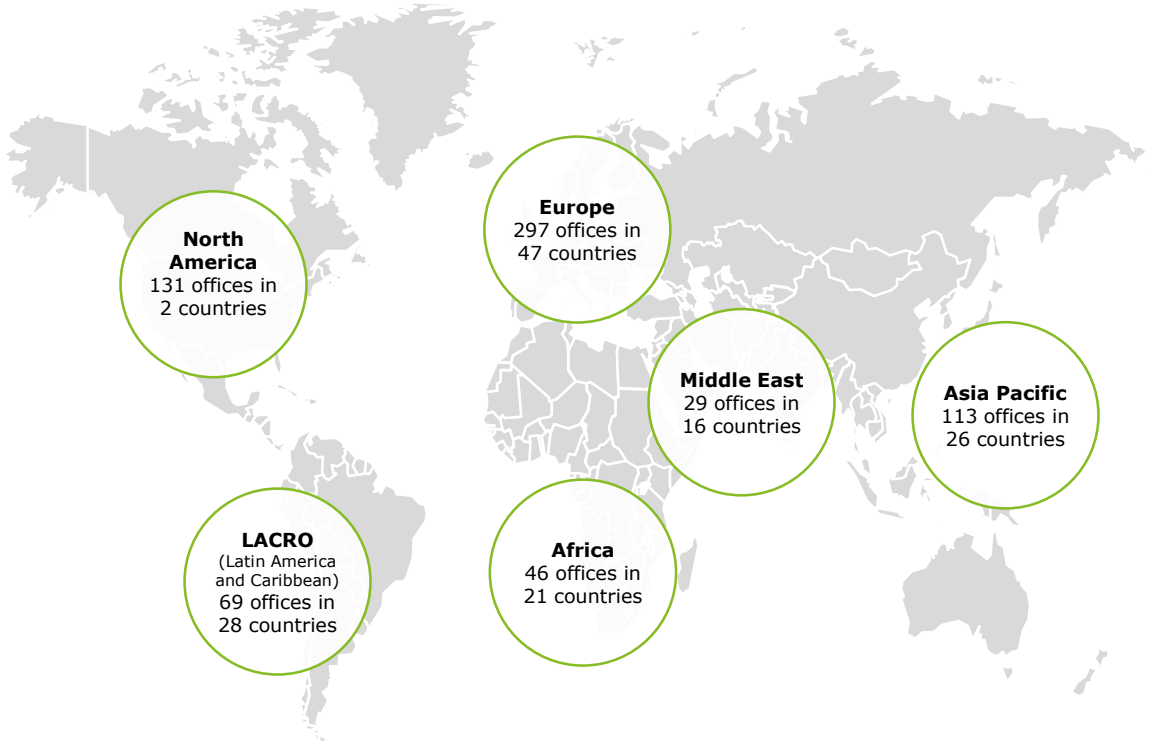
The most important external stakeholder are your data subjects. The GDPR brings increased rights to data subjects (customers, patients, citizens) and this brings procedural challenges to a controller.

Whether a data subject requests access, or correction, or restriction, or objection, or erasure or portability of their data, a good process on how to communicate and serve these data subjects is essential.

Why Deloitte?

Why Deloitte? - Global

Deloitte is the largest global professional services firm and recognised leader in the privacy and security domain



Ratio

Over 200,000 professionals in almost 140 countries share extensive knowledge and experience, which facilitates a unified approach in delivering the highest quality of services.

- More than 12,000 IT risk consultants and 3,000 security professionals worldwide;
- Analysts praise our ability to execute and tackle difficult challenges:
  - *"Deloitte's ability to execute rated the highest of all the participants."*
  - *"Deloitte shines when tackling large-scale challenges at mature, complex organizations. Customers facing such issues and looking for a vendor that will marry deep technical capabilities with strong business processes should look to Deloitte."*

Deloitte accreditations

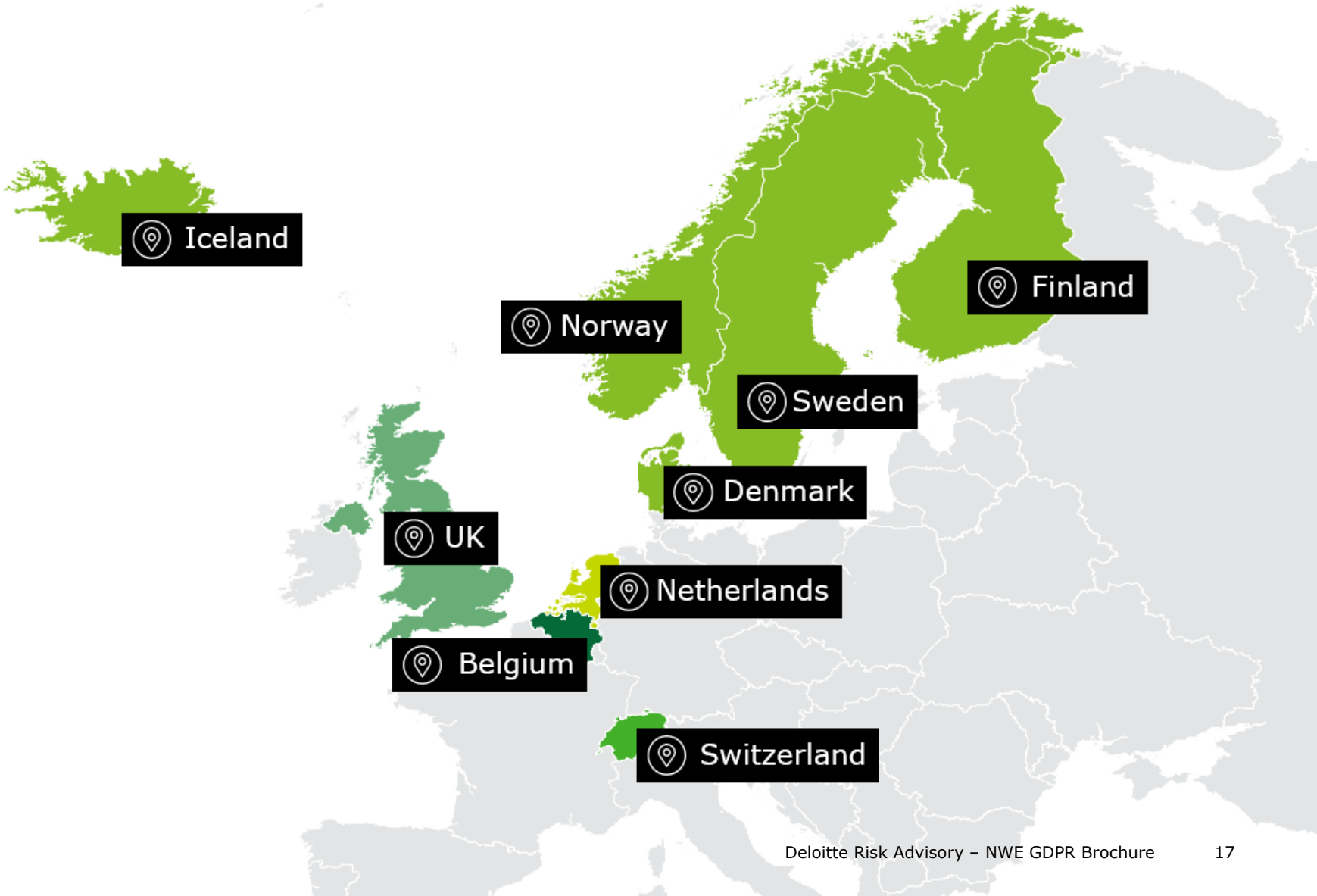
ISC^2	Over 1,100 CISSPs
ISACA	Over 2,000 certified as CISA, CISM, CGEIT
BSI	Over 150 trained lead system auditors
IAPP	Privacy certified practitioners
Specialty	Wide range of domain specific certifications
PMI	PMI certified practitioners

Why Deloitte? - NWE

Deloitte North West Europe combines the breadth and depth of capabilities of eight market leading member firms.

The privacy practice of Deloitte North West Europe

- 125 professionals from different relevant backgrounds
- Combining proven Deloitte Risk Advisory methodology with local privacy knowledge
- Certified professionals with in-depth knowledge of the General Data Protection Regulation (GDPR)
- Long tradition of cooperating on international privacy engagements
- Multi-disciplinary teams combining legal, technical and organisational knowledge and experience

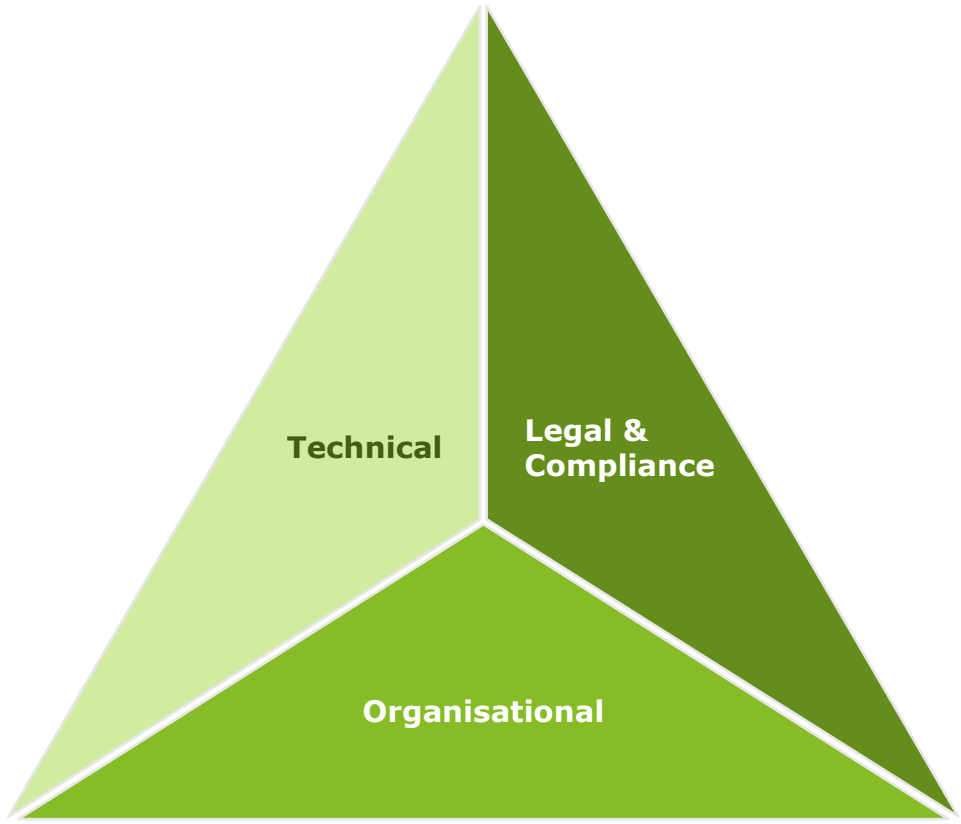


Why Deloitte?

Why our team is unique

Key focus areas

- Deloitte has an international privacy organisation and is well positioned to cross-border engagements;
- Deloitte Privacy Services is the market leader in Europe for privacy advisory services;
- In order to address privacy challenges correctly, these three focus areas **(technical, legal & compliance, and organisational)** in your organisation need to be involved. The team consists of experts on each of those fields;
- We have a wide range of services geared towards protecting privacy and our client's interests;
- We have a wealth of experience servicing clients in multiple industries;
- We are a major supplier of privacy training and education (Privacy Officer training, CIPP);
- We organize leading events on privacy such as Data with a View and GDPR Expert talks;
- Our buyers and sponsors range from CPO, CIO and CLO to strategy executives and the business.



Why Deloitte? - Our Key Privacy and Data Protection Areas

We have a dedicated team of privacy professionals, with thorough expertise in leading privacy programmes across large scale and complex organisations

Compliance and Readiness	Privacy Programmes	Technology and Digital	Risk Management	Training and Cultural Change	Cyber Security
• GDPR readiness assessment • GDPR compliance roadmap • Global privacy compliance assessment • GDPR technology impact assessment • Global compliance assessments	• Privacy programme development • Privacy strategy and roadmap development • Target operating model design and implementation • Change programme design and delivery	• Data discovery, mapping, and inventories • Privacy-by-design advice and application • Online and e-Privacy • Digital asset risk assessment and management (e.g. websites and mobile apps)	• Privacy Impact Assessment and health check • Policy analysis and design • Governance and compliance review • Third party management • Mergers and acquisitions data transfer and ownership	• Privacy risk and compliance training • Training and awareness design and implementation • Classroom and computer-based training • Cultural change programme development	• Personal data breach investigation and management • Regulatory liaison advice • Incident response and forensic investigation support • Supplier and third party management

We have experience with performing assessments of organisation's readiness based on GDPR requirements, among others.

We designed and developed group-wide privacy programmes for consumer business clients.

Our deliverables help organisations to gain a better insight in their processes regarding privacy, such as: formal reports, governance models, policies and processes, and roadmaps.

We supported the cyber response for a consumer business client which had suffered hacking and a data breach, providing advice on their customer notification and regulatory obligations.

Contact Us

Contact

Annika Sponselee

Partner | Deloitte Privacy Services

The Netherlands

Deloitte Risk Advisory
Gustav Mahlerlaan 2970
1081 LA Amsterdam
The Netherlands
+31 (0)6 1099 9302
ASponselee@deloitte.nl

Peter Gooch

Partner | Deloitte Cyber Risk Services

United Kingdom

Deloitte Risk Advisory
Hill House 1 Little New Street
London, EC4A 3TR
United Kingdom
+44 7803 003849
pgooch@deloitte.co.uk

Erik Luysterborg

Partner | Deloitte Cyber Risk Services

Belgium

Deloitte Risk Advisory
Gateway Building Luchthaven Nationaal 1 J
Zaventem, 1930
Belgium
32 497 51 53 95
eluysterborg@deloitte.com

Contact

Klaus Julisch

Partner | Deloitte Risk Advisory

Switzerland

Deloitte Risk Advisory
General Guisan-Quai 38
Zurich, 8022
Switzerland
+41 58 279 6231
kjulisch@deloitte.ch

Lars Syberg

Partner | Deloitte Risk Advisory CRS

Denmark

Deloitte Risk Advisory
Weidekampsgade 6 Postboks 1600
København C, 0900
Denmark
+45 30 93 41 34
lsyberg@deloitte.dk

Birna Maria Sigurdardottir

Partner | Deloitte Risk Advisory & Audit

Iceland

Deloitte Risk Advisory
Smáratorgi 3
Kópavogur, 20
Iceland
354-8986460
birna.maria.sigurdardottir@deloitte.is

Contact

Bjørn Jonassen

Partner | Deloitte Global Risk Advisory

Norway

Deloitte Risk Advisory
Dronning Eufemias gate 14
Oslo, 0103
Norway
+47992 27 420
bjojonassen@deloitte.no

Hannu Kasanen

Director | Deloitte Global Risk Advisory

Finland

Deloitte Risk Advisory
Porkkalankatu 24 P.O. Box 122
Helsinki, 00181
Finland
+358505311144
hannu.kasanen@deloitte.fi

Marcus Sörlander

Partner | Deloitte Global Risk Advisory

Sweden

Deloitte Risk Advisory
Rehnsgatan 11
Stockholm, 113 79
Sweden
+46 73 397 24 63
msoerlander@deloitte.se

Deloitte.