Our Services

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 a group-wide privacy programmes for a 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.

Actions to take to prepare for the GDPR

Actions to take to prepare for the GDPR

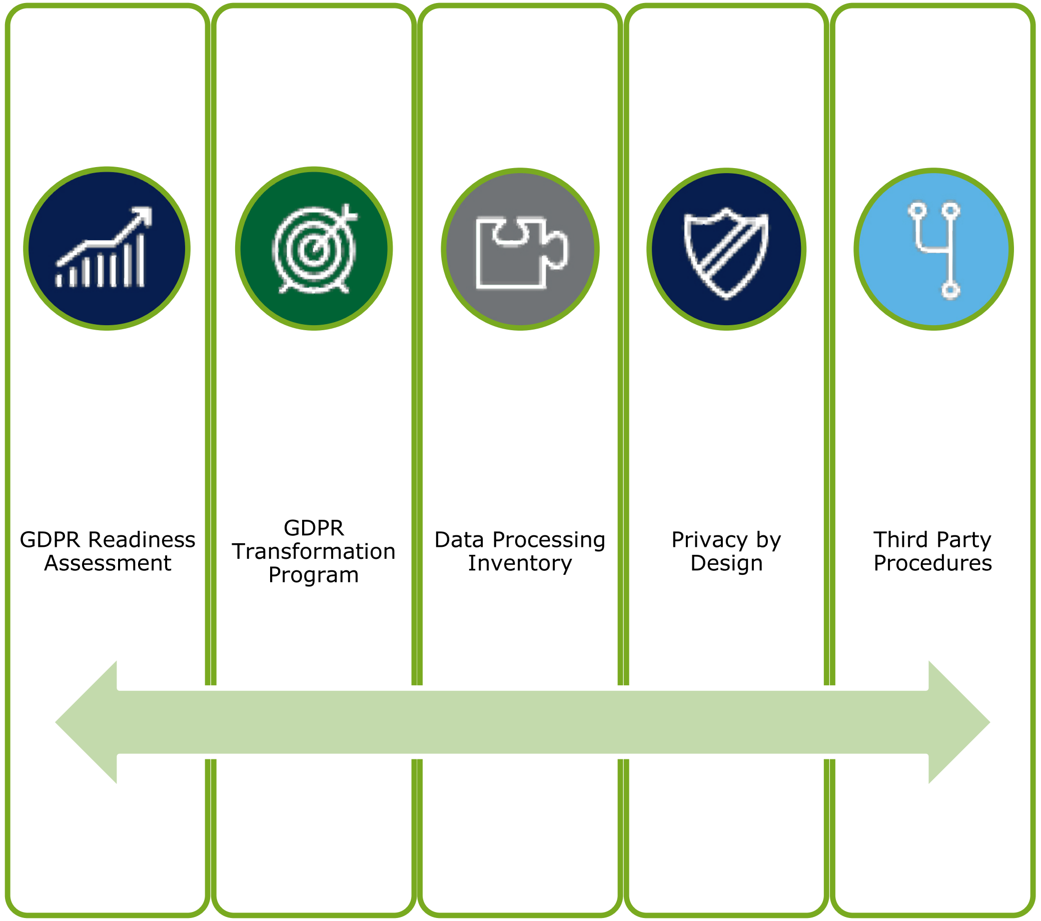
GDPR Readiness Assessment

GDPR Transformation Program

Data Processing Inventory

Privacy by Design

Third Party Procedures



GDPR Readiness Assessment

GDPR Transformation Program

Data Processing Inventory

Privacy by Design

Third Party Procedures

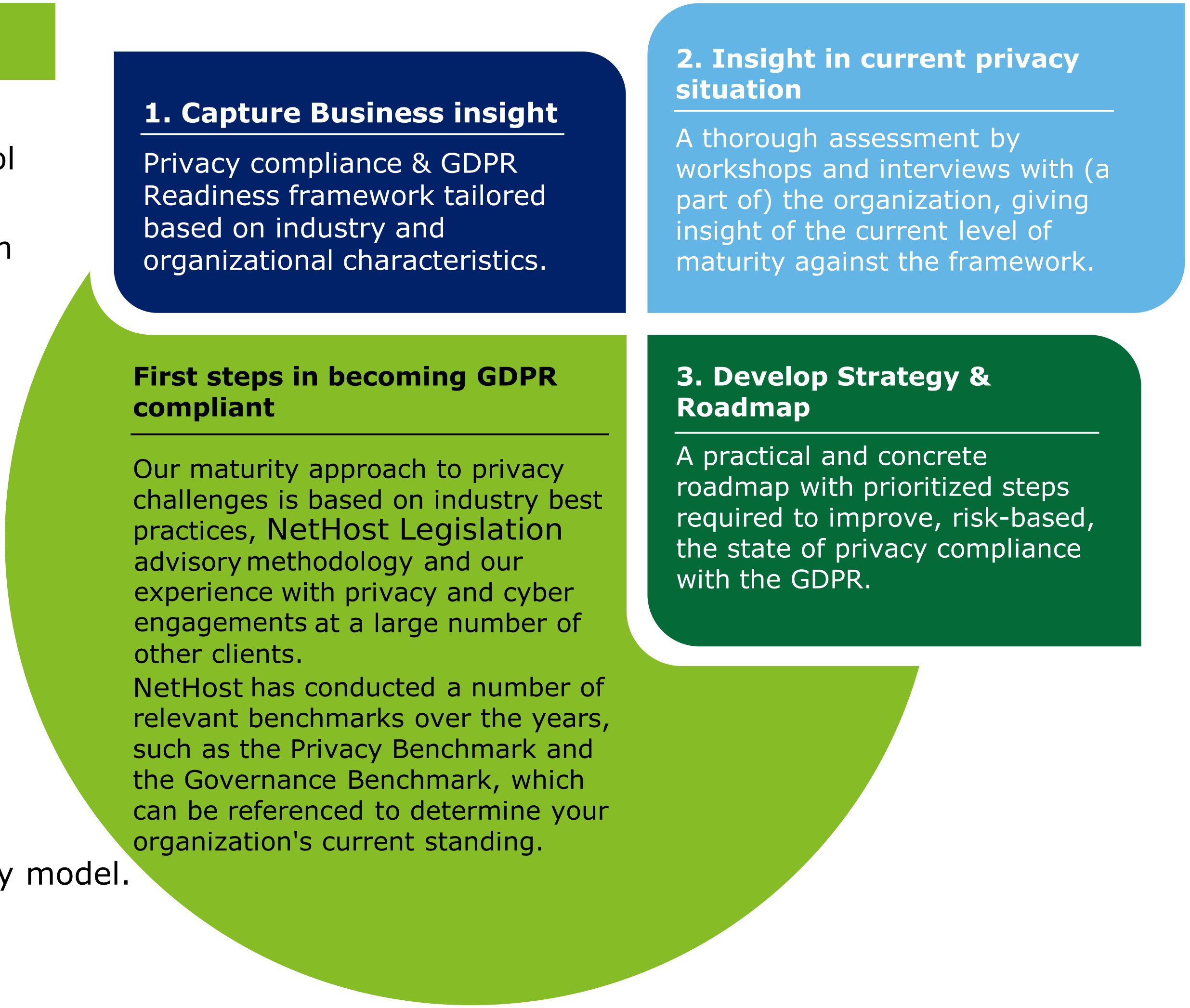
GDPR Readiness Assessment

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 organization currently stands with respect to the GDPR, the GDPR Readiness Assessment is the tool of choice. The GDPR Readiness Assessment is:

- A powerful tool, based on an existing NetHost Legislation platform to create a baseline for privacy;
- Part of the cyber tooling suite, potential to incorporate into your broader cyber strategy and roadmap;
- Used by NetHost Legislation 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 organization currently is, using the NetHost Legislation privacy and data protection maturity model.



1. Capture Business insight

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

2. Insight in current privacy situation

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

First steps in becoming GDPR compliant

Our maturity approach to privacy challenges is based on industry best practices, NetHost Legislation advisory methodology and our experience with privacy and cyber engagements at a large number of other clients.

NetHost 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 organization's current standing.

3. Develop Strategy & Roadmap

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

Privacy by Design

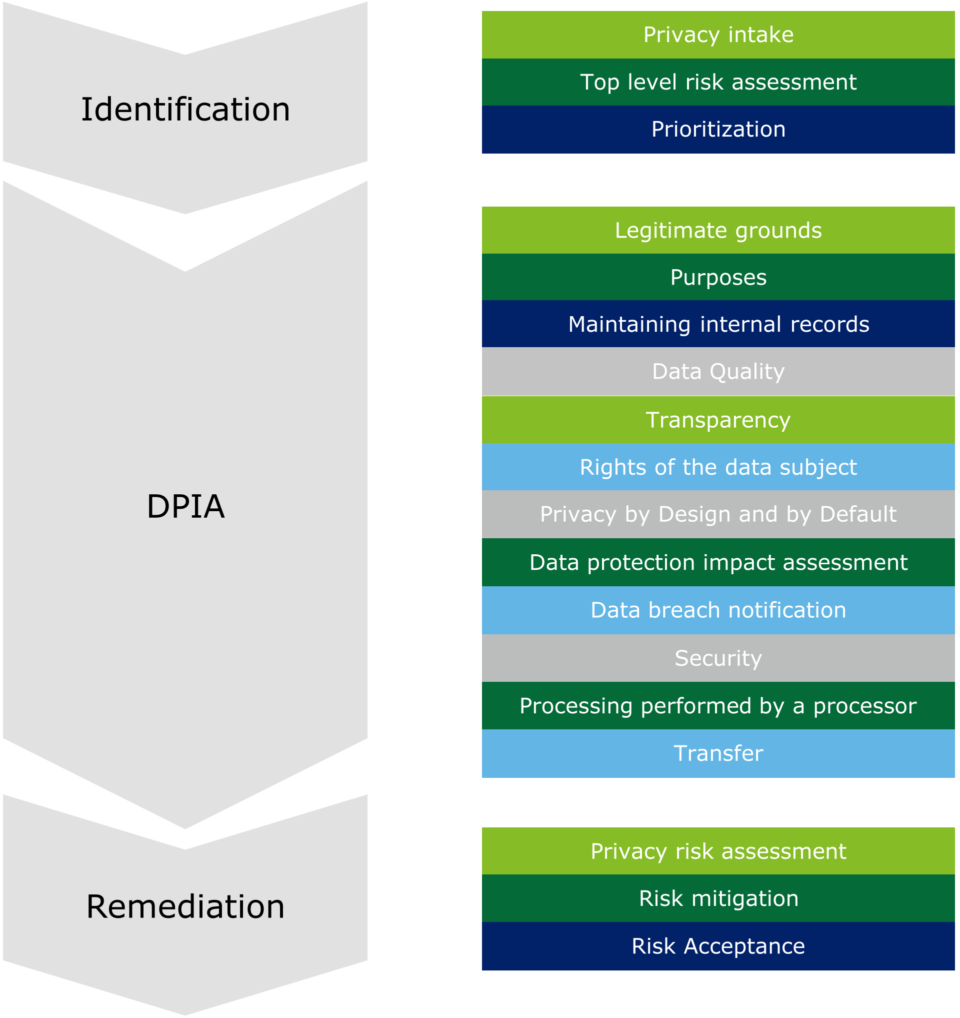
Embedding privacy into your project methodology by assessing privacy risks in an early stage

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 organization is done through a robust Privacy by Design (PbD) approach;
- Data Protection Impact Assessments (DPIAs) are based on the GDPR and are a proven and effective tool to assess privacy risks;
- A PbD approach consists of a number of elements: a PbD process, DPIA method, and a remediation framework:
  - 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 privacy by design and makes sure impact can be reduced and risks mitigated or accepted.

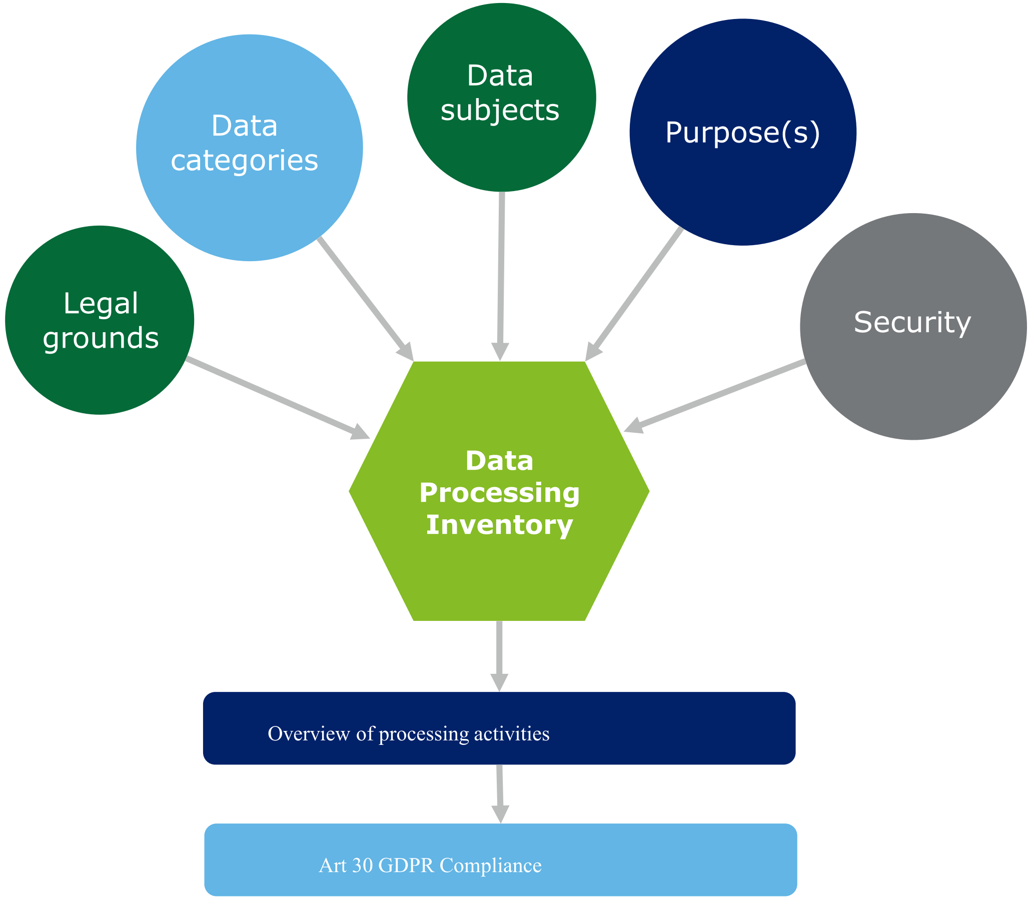


Data Processing Inventory

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 legal grounds, purpose(s), categories of data, retention period and conducted risk analysis.
- 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 organization. Having an inventory is essential for your oversight of processing activities and is a mandatory element of GDPR compliance.
- The inventory allows your organization to demonstrate awareness of its obligations as a data controller, including keeping of records of processing activities.
- Finally, knowing which personal data the organization processes mitigates the risk of unidentified data breaches.

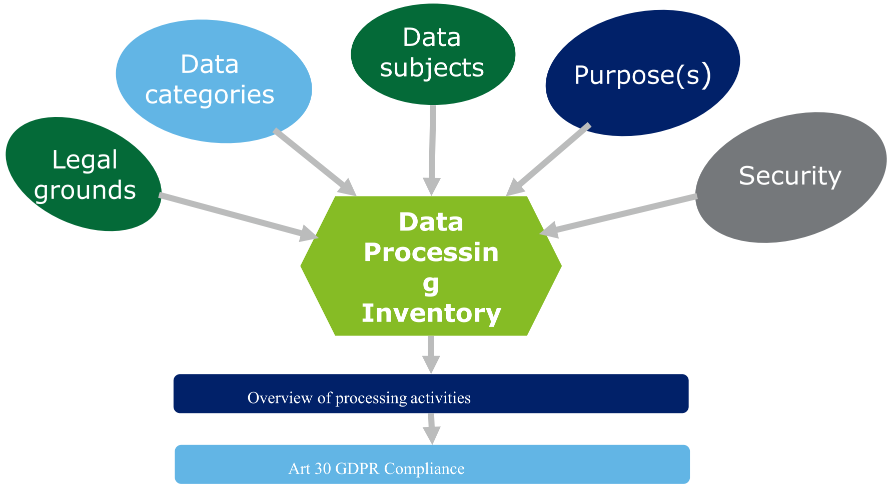


Data Processing Inventory

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 legal grounds, purpose(s), categories of data, retention period and conducted risk analysis.
- 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 organization. Having an inventory is essential for your oversight of processing activities and is a mandatory element of GDPR compliance.
- The inventory allows your organization to demonstrate awareness of its obligations as a data controller, including keeping of records of processing activities.
- Finally, knowing which personal data the organization processes mitigates the risk of unidentified data breaches.



Data categories

Data subjects

Purpose(s)

Legal grounds

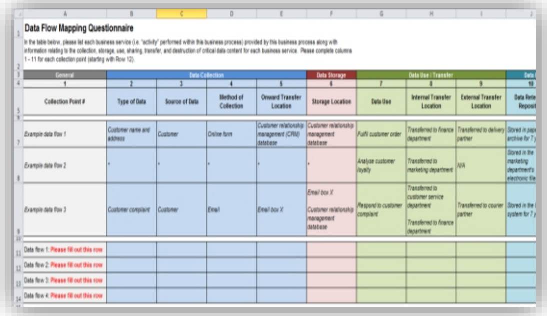
Security

Data Processin g Inventory

Overview of processing activities

Art 30 GDPR Compliance

In data mapping, there are two stages: the data capture template and the data map flowchart.

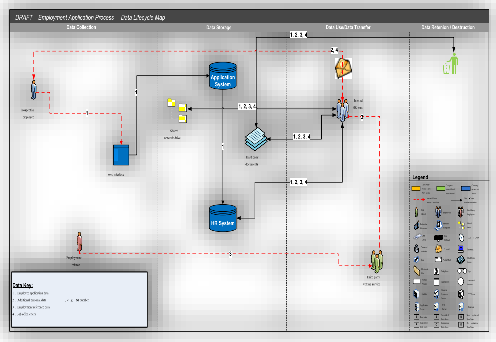


Data Flow Mapping Questionnaire

In the table below, please list each business service (i.e. "activity" performed within this business process) provided by this business process along with information relating to the collection, storage, use, sharing, transfer, and destruction of critical data content for each business service. Please complete columns 1 - 11 for each collection point (starting with Row 12).

General	Data Collection				Data Storage	Data Use / Transfer			Data
1	2	3	4	5	6	7	8	9	10
Collection Point #	Type of Data	Source of Data	Method of Collection	Onward Transfer Location	Storage Location	Data Use	Internal Transfer Location	External Transfer Location	Data Rete Reposit
Example data flow 1	*Customer name and address*	*Customer*	*Online form*	*Customer relationship management (CRM) database*	*Customer relationship management database*	*Fulfil customer order*	*Transferred to finance department*	*Transferred to delivery partner*	*Stored in pap archive for 7 y*
Example data flow 2	*	*	*	*	*	*Analyse customer loyalty*	*Transferred to marketing department*	*N/A*	*Stored in the marketing department's electronic file*
Example data flow 3	*Customer complaint*	*Customer*	*Email*	*Email box X*	*Email box X* *Customer relationship management database*	*Respond to customer complaint*	*Transferred to customer service department* *Transferred to finance department*	*Transferred to courier partner*	*Stored in the system for 7 y*
Data flow 1: Please fill out this row									
Data flow 2: Please fill out this row									
Data flow 3: Please fill out this row									
Data flow 4: Please fill out this row									

Data capture template



Data Map flowchart

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 (DPAs)

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

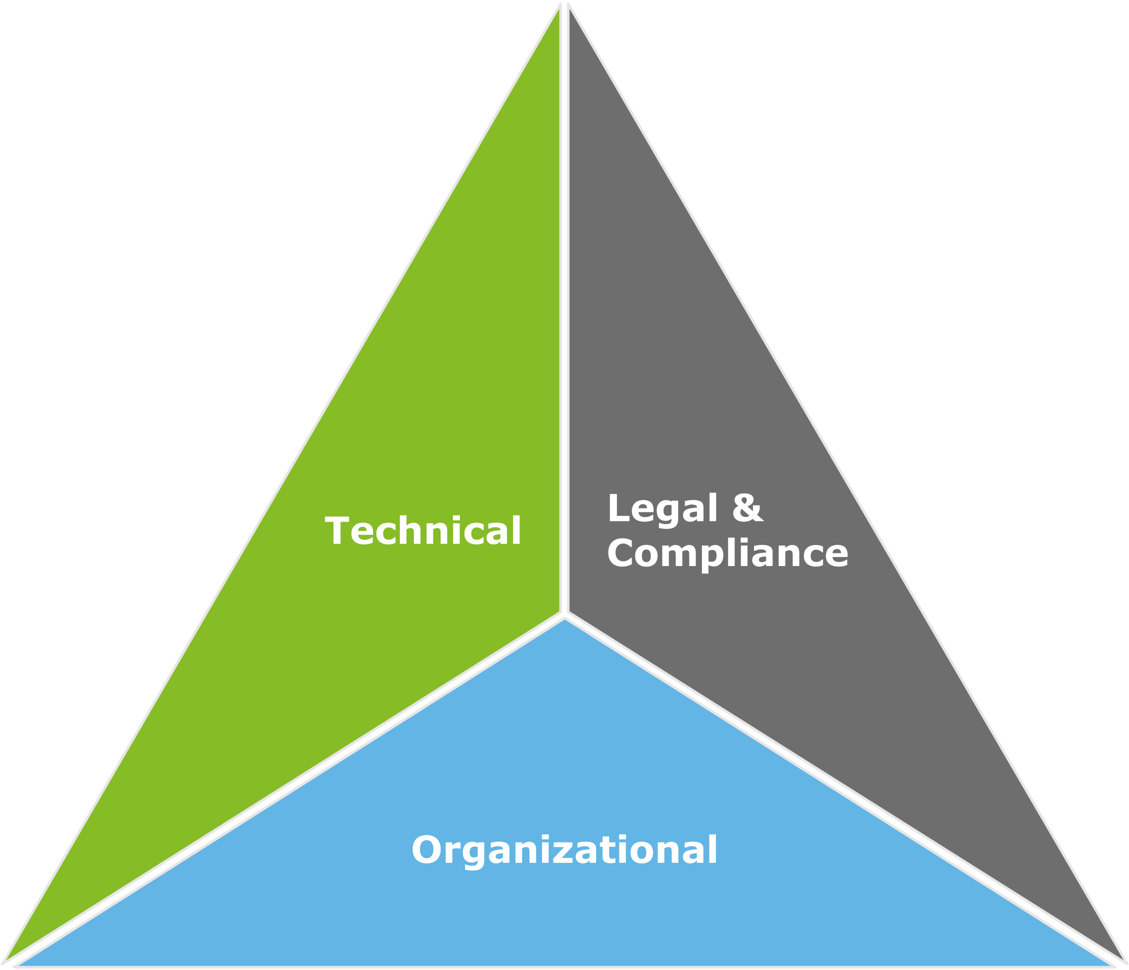
The most important external stakeholder are your data subjects. The GDPR brings increased rights to data subjects (customers, patients, citizens) and this brings procedural challenges to a controller. Whether a data subject requests access, erasure or portability of their data, a good process on how to communicate and serve these data subjects is essential.

NetHost Legislation vision on Privacy

Why our team is unique

Key focus areas

- NetHost has an international privacy organization and is well positioned to cross-border engagements;
- NetHost 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 organizational)** in your organization 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.


Technical
Legal & Compliance
Organizational