

PRIVACY, DATA PROTECTION & THE GDPR



Secura has nearly two decades of experience in helping her customers protect their data. As a part of our Advisory & Audit service line, we offer a number of services dealing with data protection and privacy. If you are a data protection officer, or otherwise responsible or accountable for privacy and data protection, you will find the relevant services we offer in this factsheet.

IN CONTROL WITH SECURA

Secura has worked in information security and privacy for nearly two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing services varying in depth and scope.

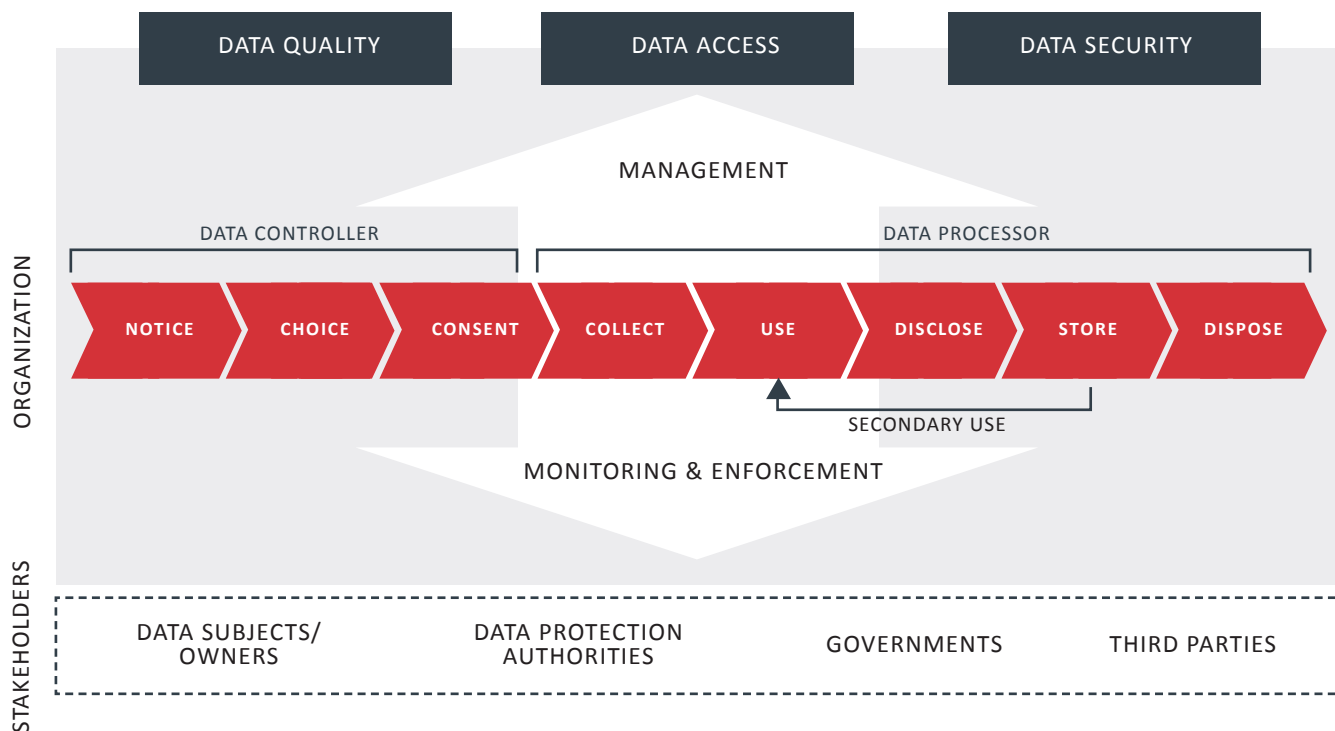
OUR CHANGING DATA

Throughout the life cycle of information, it's attributes relating to privacy and data protection change. Something can be secret today, and public tomorrow. For instance, when a person deceases, his previously confidential medical information is no longer bound by the same protections for patient data as before. Data classification and data security (and by extension, security technologies) play a large role in the proper life cycle management of information.

In many countries, there are laws and regulations in place to protect the privacy of people and the confidentiality of data. And for Europe, the GDPR is of course active now. Secura offers several services around the GDPR and privacy:

- GDPR Training (Overview & In-Depth)
- GDPR Implementation Support
- (D)PIA
- Privacy Assessment / Gap analysis
- PCF Audit





GDPR TRAINING

Designing and implementing sufficient controls to ensure continuous compliance is quite a challenge. It is essential for management to get a clear overview, and to practice how to deal with this major change in regulation, which has impact on all levels of the organization. During our three-day course we will guide you through the GDPR and pay attention to some specific items in day two and three:

- The role of the Data Protection Officer (DPO)
- Performing a Data Protection Impact Assessment (DPIA)
- Privacy by design and default
- Demonstrating compliance

After the training you will gain an understanding of the main topics within the GDPR, and how these interact with each other. You will have a idea on how to determine the impact the GDPR has on your organization, DPIA's the role of the DPO, the risks involved, and guidelines on how to address these risks.

GDPR IMPLEMENTATION SUPPORT

Secura offers support with GDPR implementation, from creating awareness to verifying if the GDPR has been implemented correctly, and designing the processes around data protection itself. Our consultants can provide:

- **Training and awareness** (see above)
- **GDPR GAP Analysis**
 - What is the current implementation status?
 - What needs first attention?
 - Action Plan and follow-up.
- **Information Security Management System (ISMS) implementation including privacy aspects**
 - Policy development;
 - Plan-Do-Check-Act (PDCA) cycle activities;
 - Risk and Impact assessment process implementation;
 - (Internal) audits regarding compliance status;
 - Data classification process implementation.
- **Review and testing:**
 - Design Review;
 - Vulnerability Analysis and Penetration testing;
 - Source code analysis.
- **Data Protection Officer (DPO) as-a-service:**
 - For smaller organisations, or organisations that lack the skills and knowledge, we provide a (part-time or full-time) DPO.

In order to provide a complete covering result, our Consultants address all the relevant aspects being People, Process, Organization and Technology.

(D)PIA

Mandatory (periodic) Impact Assessments are a core element of the GDPR and other privacy frameworks. A Data Protection Impact Assessment (DPIA) or Privacy Impact Assessment (PIA) is necessary for inventorying the information assets, the impact on the organisation and the person the data relates to and determining the necessary controls. Secura offers these assessments for every size organisation and for every sector. Our impact assessments follow the international standard for the execution of these types of projects. Our experienced and certified specialists and consultants will provide their knowledge and insight in these matters. A DPIA contains at least the following aspects:

- a description of the operations and the purposes of the processing of personal data
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the rights and freedoms of data subjects;
- the (security) measures and mechanisms to ensure the protection of personal data;
- how you comply to the GDPR.

PRIVACY ASSESSMENT AND GAP ANALYSIS

When a full privacy audit has too much impact on an organisation, it can be helpful to approach these issues from a more general standpoint. If your goal is simply to know where you stand, and what you would need to do to become fully GDPR compliant, then Secura can perform a Privacy Assessment or a GAP analysis. The privacy assessment will tell you what your current status is, while identifying the most important risks, both to your organisation and to the personal data being processed. The GAP analysis goes a little further, and also identifies the specific aspects that need to be addressed in order to become GDPR compliant.

Both assessment types are of course nearly always a part of any larger GDPR implementation project. They deliver clear, accurate and actionable recommendations and allow your organisation to focus on the most important issues first.





PRIVACY AUDIT PROOF™

The core of privacy assurance is a privacy audit. The results of such an audit will demonstrate the fact that your organization, service or product takes responsibility regarding the privacy of user's data and complies with certain criteria.

Secura uses a clear set of requirements, the **NOREA Privacy Control Framework (PCF)**, that our auditors use in order to conduct meaningful assessments. The requirements are designed such that they are in line with the GDPR regulation. This PCF methodology provides privacy controls addressing a wide range of domains, for example:

- Management: existence of internal policies regarding privacy principles and applicable laws and regulations
- Notice: transparency in informing the data subjects of the existing policies, requirements and practices
- Choice and Consent: enforcement of the data subject's consent before processing personal data
- Collection: limitation of collected data only to necessary purposes

- Usage, storage and disposal: requirements for retention, use limitation, disposal and anonymization of collected data
- Data access and data quality: requirements for data access, correction, portability and completeness
- Disclosure: requirements for data disclosure to third parties
- Data security: requirements for secure access, transmission and storage of data
- Monitoring and Enforcement: continuous review of compliance with applicable laws and regulations and periodic assessment of privacy processes and controls

As a result of the PCF audit, Secura will provide an **Assurance Report**, in line with the ISAE 3000 international assurance standard. This assurance report will be signed off by a certified auditor (RE), providing you with an internationally recognized means for demonstrating the compliance of your privacy principles. On request the report can be used to obtain the **certificate Privacy Audit Proof™**.



INTERESTED?

Would you like to learn more about our services?
Please do not hesitate to contact us.

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

Follow us on   

T +31 (0)40 23 77 990
E info@secura.com
W www.secura.com