Design by Privacy: A holistic approach to privacy by design

Erik Luysterborg (EMEA Data Protection & Privacy Practice Lead)
Jan Vanhaecht (EMEA IAM Practice Lead)
Privacy Café, Mechelen, 14th December 2016
Introduction

Deloitte and Privacy: A Holistic, experience-based team, driven by pragmatism and best practices

We form a **multidisciplinary**, highly **motivated** team of over **60 security and legal professionals in Belgium**. We have made it our priority to turn your data protection and privacy challenges (incl. GDPR (General Data Protection Regulation) forthcoming ones) into tested, modular and pragmatic solutions enabling you to manage your risks successfully.

---

**Legal**

We are a strategic advisor of private-public sector, bringing forward pragmatic solutions

---

**Technology**

We have the technology experts to assist you with GDPR’s technological aspects

---

**Operational**

We have cyber strategy, readiness, data breach and data leakage experts

---

A few **recent** projects we assisted our clients include:

- Third party due diligence project for cloud services
- Customer Privacy Statement and Benchmarking / Customer Transparency Strategy
- GDPR/privacy quick scans (incl. roadmap for remediation)
- Act as a data protection helpdesk or as a external data protection officer (dpo as a service)

---

**Key facts**

- Center of excellence for privacy and security services in Belgium and worldwide
- Unique holistic value proposition by combining legal, operational and technical expertise
- Real cooperation with Deloitte Offices abroad with strong credentials building the Network of Security and Legal Professionals
- Local GDPR experts

---

© 2016 Deloitte Belgium

Privacy Café - 14/12/2016

Design by Privacy: A holistic approach to privacy by design
• Technology today is allowing companies to gain important competitive advantages through cross-border and inter-departmental sharing of (personal) data.

• Privacy cannot be tackled anymore as a mere legal, compliance or IT issue. It requires a fresh, more holistic approach combining all of the above aspects in a pragmatic manner in order to ensure effective privacy by design.

• It is in this context that a General Data Protection Regulation (GDPR) has been approved, with the objective to harmonize the current fragmented legal framework for data privacy across Europe and introduce a high level of protection for individuals.

• The GDPR and its privacy by design requirements introduce new operational challenges for organizations: new requirements and obligations for legal and compliance functions, changes to the ways in which technologies are designed and managed, clear information management and renewed emphasis on organizational accountability requiring robust privacy (data) governance.

• In fact the GDPR requirements will ace far reaching consequences in that many processes will need to be adapted structurally to comply with privacy by design principles or in other words, their design will be truly driven by privacy requirements.
Introduction
Short Recap: Scope of the General Data Protection Regulation (GDPR)

What will change against the former 1995 EU Data Protection Directive?

- **Broader territorial scope**: Applies to players not established in the EU but whose activities consist of targeting data subjects in the EU.
- **Enforcement**: Data Protection Authorities will be entitled to impose fines ranging between 2 to 4% of annual turnover and increased powers.
- **Accountability**: Explicit obligation on controller AND processor to demonstrate their GDPR compliance (e.g., data protection officer, privacy impact assessments (PIA)).
- **Expanded definitions**: Personal data now explicitly includes location data, IP addresses, online and technology identifiers.
- **Data subjects rights**: Reinforced rights: Access, rectification, restriction, erasure, objection to processing; no automated processing and profiling, data portability.
- **Consent**: Spelled out more clearly and focus on ability of individuals to distinguish a consent. Need for affirmative action.
- **Data breach notification**: Report a personal data breach to the Data Protection Authority within 72h.
- **One-stop shop**: Data Protection Authorities (DPA) of main establishment can act as lead DPA, supervising processing activities throughout the EU.
- **International data transfers**: Binding Corporate Rules as tools for data transfers outside the EU and EEA are now embedded in law.
Design by Privacy: A holistic approach to privacy by design

Contents

- Legal context and framework
- Software developers view on Design
- Practical approach for Privacy aware Design
- Lessons learned
- Conclusion: Some food for thought
Privacy by Design: EU Legal Context
Concept in the new GDPR

Art. 25 (1)
Privacy by Design

- implement technical and organizational measures
- at time of determination of the means of processing & at the time of processing itself

Art. 25 (2)
Privacy by Default

- only personal data which are necessary for each specific purpose are processed
- amount of data, the extent of their processing, storage period and accessibility
## Privacy by Design: Framework

### Why choose Privacy by Design?

#### Concept

- Privacy by Design is an internationally recognized privacy standard that has been endorsed globally by Data Protection Authorities and Privacy Commissioners, since 2010.
- It means building privacy into the design, operation and management of IT systems, networks and business processes.

#### Value Proposition

- Treats privacy as a competitive advantage to earning customer loyalty and trust.
- Enables wider adoption of new technologies.
- Minimizes risk of privacy infractions, security breaches and associated reputational impacts.
Privacy by Design: European Data Protection Supervisor
Opinion 7/2015

A Call for Transparency, User Control, Data Protection by Design and Accountability

“Technology and privacy-friendly engineering can play a key role in ensuring that transparency and user control, …, will become a reality. Laws, regulations, contractual terms, internal procedures, and privacy policies, while important, will not suffice on their own. Individuals need to be offered new, innovative ways to be informed about what happens to their data, and to exercise control over their data. This requires innovative and privacy-friendly engineering as well as privacy-friendly organizational arrangements and business practices.” Nov. 19th, 2015

✓ Strike the right balance between privacy by policy (focuses on process and people) with privacy by architecture (focuses on technology and architecture design).
Privacy by design and GDPR: A helicopter view

The requirements from the GDPR fall into five areas

1. Data Governance
The tone on the top, policies, roles, responsibilities, and organizational structures support the protection of individuals’ privacy

2. Data Subject Rights
Controllers gives individuals ("data subjects") control over what data is processed about them and for what purpose

3. Security of Personal Data
Personal data is processed securely; authorities and where applicable data subjects are notified of high-risk breaches

4. Data Transfers
Legal and procedural controls are in place to ensure the adequate protection of personal data by 3rd parties

5. Data Protection Principles
Business and HR processes are such that the processing of personal data is lawful, purpose-limited, and transparent to the data subject

GDPR requirements that are generally implemented centrally and can be assessed once for the entire company

GDPR requirements that are generally implemented by each HR and Business Process separately and consequently, must be assessed on a process-by-process basis
Privacy by design and GDPR: Need for a pragmatic, holistic approach
Protect yourself from common pitfalls

Data Protection Principles
- Accountability
- Storage limitation
- Purpose limitation
- Lawfulness
- Data minimisation

Data Governance
- Risk methodology
- Third party management
- Privacy Impact Assessments

Privacy by Design/by Default
- Roles & responsibilities
- Audits
- International transfers
- Training & awareness

Data Subject Rights
- Transparency
- Handling requests
- Automated decision-making & profiling

Strategy & processes
- Limited or no formal accountability
- Incident/breach management

Technology
- Documentation
- Heterogeneous approach
- Lack of coordination and oversight

Secure SDLC
Information Tagging
Access Controls
Database security
Legal & Policies
Information Classification
© 2016 Deloitte Belgium
Design by Privacy: A holistic approach to privacy by design

Contents

- Legal context and framework
- Software developers view on Design
- Practical approach for Privacy aware Design
- Lessons learned
- Conclusion: Some food for thought
GDPR is not only about legal aspects of data protection
GDPR is not only about technical aspects of data protection

GDPR calls for a combined approach

Design by Privacy: A holistic approach to privacy by design
"Privacy on all layers" approach

**Governance, organisation & people**
- Legal framework
  - Privacy Statements
  - Roles & Responsibilities

**Processes**
- Data Lifecycle Management
  - Requirements gathering
  - & privacy-aware processes
- Information Classification
  - Information Tagging
- Data (Lifecycle) Governance
- Data(base) security
  - Data Leakage Protection
  - Data Lifecycle Management

**Data**

**Technology**

**Vision**

**Policies**

**Procedures**

**Instructions**
Design by Privacy: Practical approach for Privacy aware Design
Secure Software Development Lifecycle

SDLC is the Software Development Lifecycle: It defines the tasks in each step of the software development process.

Secure software is a continuous concern for all organizations.

SSLDC will cause an overall *risk reduction* for the organization.

SSLDC causes *early detection of vulnerabilities* in an early stage of the development lifecycle.

Secure SDLC
*Develop and maintain software in a consistent and efficient way with predefined security quality, in line with the organizational risks.*

SSLDC will raise *awareness* of security considerations by stakeholders.
Design by Privacy: Practical approach for Privacy aware Design
Software Development Lifecycle deliverables

**Gate 1**
Capture high-level business requirements and establish solution vision.

- Vision
- Roadmap
- Business objectives/drivers
- Business impact risk assessment
- High level data model
- High level process model (L1/L2)
- High level component model

**Gate 2**
Formalize functional requirements and conceptual design of solution.

- Operational KGI’s & KPI’s
- Conceptual data model
- Process flows (L3)
- Use Cases (Unified Process style)
- Data flow model
- Deployment model
- UX design

**Gate 3**
Detailed technical design and solution development/product installation & configuration.

- Detailed Domain/object model
- Detailed workflows (L4/L5)
- User stories
- API definitions
- Detailed UI/screenflow design
- Network design
- Code & Configuration

**Inception**
- Vision
- Roadmap
- Business objectives/drivers
- Business impact risk assessment
- High level data model
- High level process model (L1/L2)
- High level component model

**Elaboration**
- Operational KGI’s & KPI’s
- Conceptual data model
- Process flows (L3)
- Use Cases (Unified Process style)
- Data flow model
- Deployment model
- UX design

**Build**
- Detailed Domain/object model
- Detailed workflows (L4/L5)
- User stories
- API definitions
- Detailed UI/screenflow design
- Network design
- Code & Configuration

**Operations**
- Standard operating procedures
- Installation documentation
- (Data) Migration documentation
- Upgrade procedures
- Backup-procedures
- Monitoring integration

Roll-out and run the solution.
Design by Privacy: Practical approach for Privacy aware Design
Software Development Lifecycle security & privacy control deliverables

Gate 1
Capture high-level business requirements and establish solution vision.
- Privacy Impact Assessment
- Confidentiality Impact Assessment
- Data Integrity Impact Assessment
- Availability Impact Assessment
- High Level Security Controls Checklist

Gate 2
Formalize functional requirements and conceptual design of solution.
- Security & Privacy aware data modelling
- Security aware process modelling
- Security Services integration design (logging/proxying/authentication/...)
- Low Level Security Controls Checklist

Gate 3
Detailed technical design and solution development/product installation & configuration.
- During technical design:
  - Segregation of responsibility
  - Security on all layers
  - Use of code (style) checkers
  - Define anti-patterns & patterns
  - External code-review
- During continuous/nightly build:
  - Automated code analysis in nightly build environment
  - Vulnerability assessments

Operations
Roll-out and run the solution.
- Data retention & backup policies
- Security monitoring
- Security Configuration management
- Key lifecycle management
- Privileged access management
- Account lifecycle management
- Security Patch management
- Security Release management
- Vulnerability management
- Availability management

Inception
Elaboration
Build
Operations
Legal context and framework

Software developers view on Design

Practical approach for Privacy aware Design

Lessons learned

Conclusion: Some food for thought
Lessons learned
Need for Privacy Champions

The privacy champion role should be filled by SMEs from the project teams

Responsible for the identification, negotiation, acceptance and tracking of minimum security requirements

Act as the ‘advocate’ of privacy for development team

Responsible for coordinating and tracking privacy risks for the project

Responsible for reporting status to the privacy architect and to other relevant parties (for example development and test leads) on the project team

Privacy champions should be coached by DPO and help enforce organization-wide privacy-by-design standards and guidelines

A Privacy Champion helps to increase Privacy aware design among analysts and developers and raise awareness of the importance of privacy.
Lessons learned
Alignment is key Business – IT – Risk & Compliance – Legal

Ensure buy-in Board & Senior Management

Involve key stakeholders: DPO, executive responsible for privacy compliance, privacy liaisons, ICT (both developers & operations), Risk, Legal, Compliance, process/product/service owners, end users, ...

Look for allies within your organization, e.g. Finance, Procurement (“gateway” functions)

Clear definitions: common understanding & avoiding “scope creep”

Avoid “silo-approach”: important to understand the entire data life cycle

Clear deadlines required for follow-up remediation actions

Privacy is not a show stopper but a business enabler

Think business in a privacy compliant way (“no, not that way” instead of “no”)

Talk business/operational (avoid legalese)

Focus on the added value of Privacy by Design approach:

✓ Board: avoiding sanctions and safeguarding good reputation
✓ Business: cost saving as it avoids projects being delayed or stopped in a later stage
✓ Marketing & Sales: sales argument of privacy-compliant organization
✓ Compliance: helps you comply with duties you have already got
Design by Privacy: A holistic approach to privacy by design

Contents

- Legal context and framework
- Software developers view on Design
- Practical approach for Privacy aware Design
- Lessons learned
- Conclusion: Some food for thought
Conclusion: Some food for thought

Conclusion

- Privacy by Design will become mandatory (General Data Protection Regulation)
- No common standard (yet), but minimum (good practice) requirements
- Tailor Privacy by Design process to your organization
- Increase value by embedding within existing risk management processes
- Use Privacy by Design to enhance privacy awareness within your organization
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 225,000 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.

© 2016 Deloitte Belgium