

Privacy by Design

Data Protection by Design



ADaCoR (Advanced Data Collection and Risks)
Industry Workshop

21. April 2016

Alain Herrmann
IT & New technologies

- **Personal Data (GDPR)**
- 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- Popular (substantive) Privacy Definitions:
 - “the right to be let alone” => focusing on freedom of intrusion
 - “the right to informational self-determination”
 - ⇒ allowing individuals to control, edit, manage and delete information about themselves and decide when, how and to what extent its information is communicated to others.

(Data Privacy / Data Protection is derived from the right to informational self-determination)

- Concept of PbD:
 - A philosophy in which privacy is embedded into the technology itself during the development, such that privacy and data protection becomes part of designers’ original goals.

“Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves” (Ch. Fried (1968), Privacy. In: Yale L.J.)

Protection of natural persons with regards to the processing of personal data



Impact on individuals

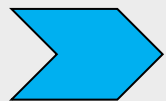


Impact on organizations

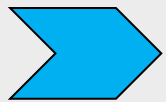
Personal Data Protection



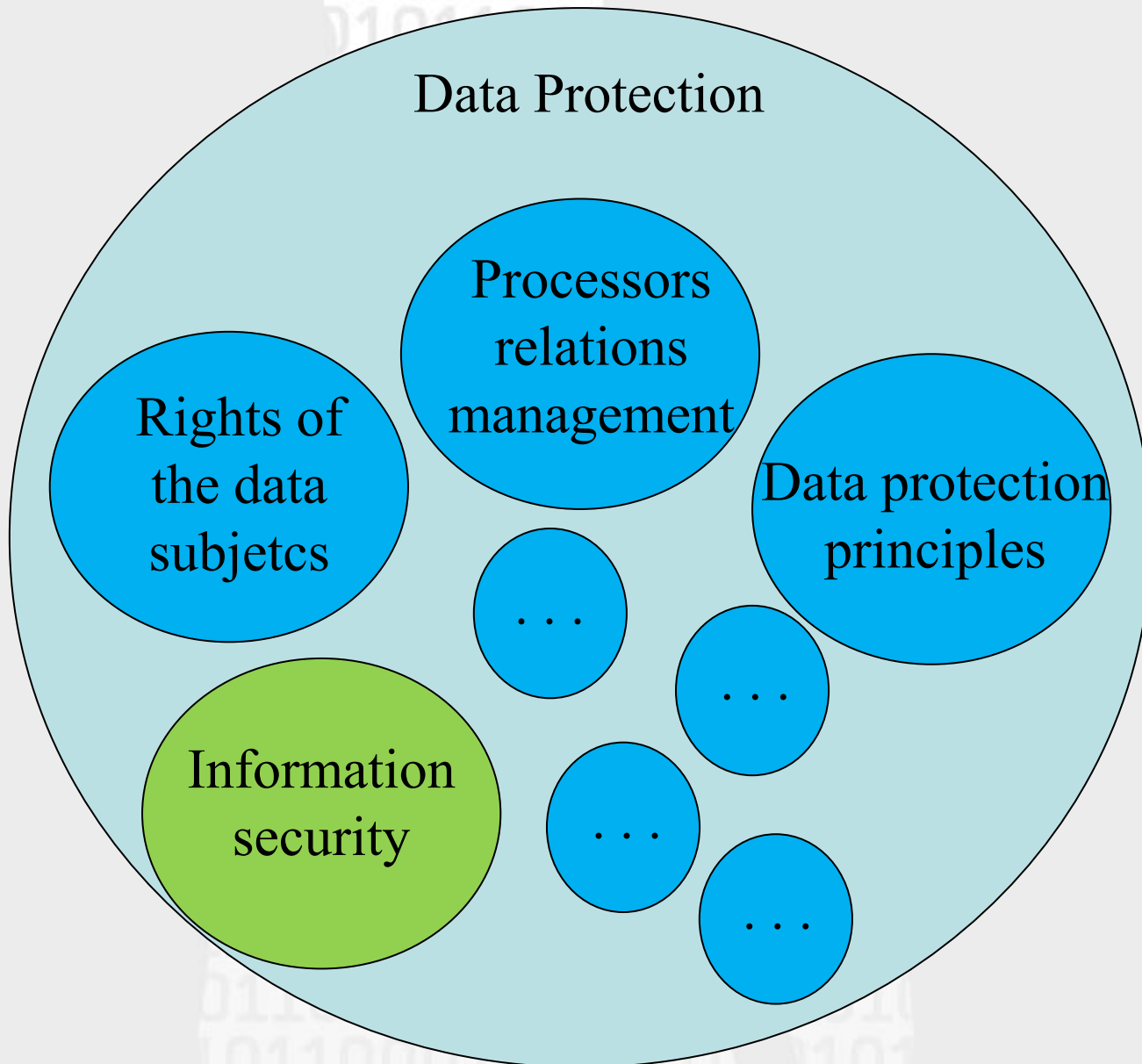
Information Security



An information system can be perfectly secured, but the personal data processing can be illegal or non compliant with the data protection legislation



Information security = 1 element of data protection



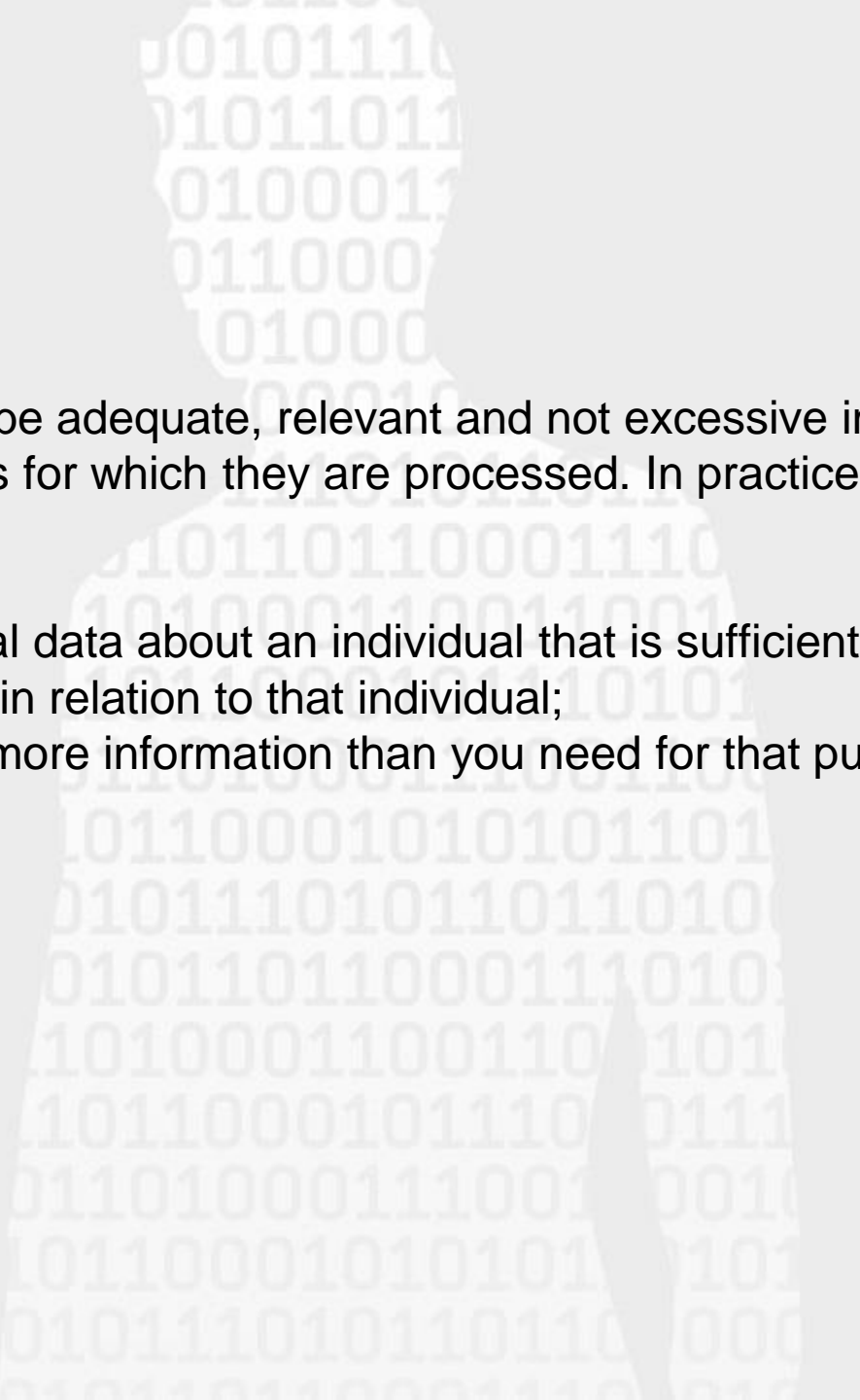
- Personal data shall be processed fairly and lawfully

In practice, it means that you must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people’s personal data only in ways they would reasonably expect; and
- make sure you do not do anything unlawful with the data.

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes:

- In practice, the second data protection principle means that you must:
- be clear from the outset about why you are collecting personal data and what you intend to do with it;
- comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
- ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

A faint silhouette of a person is centered in the background, overlaid with a pattern of binary code (0s and 1s). The person's head is at the top, and their body extends downwards. The binary code is scattered across the silhouette and the surrounding white space.

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. In practice, it means you should ensure that:

- you hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual;
- you do not hold more information than you need for that purpose.

Personal data shall be accurate and, where necessary, kept up to date.
To comply with these provisions you should:

- take reasonable steps to ensure the accuracy of any personal data you obtain;
- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to update the information.

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. In practice, it means that you will need to:

- review the length of time you keep personal data;
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

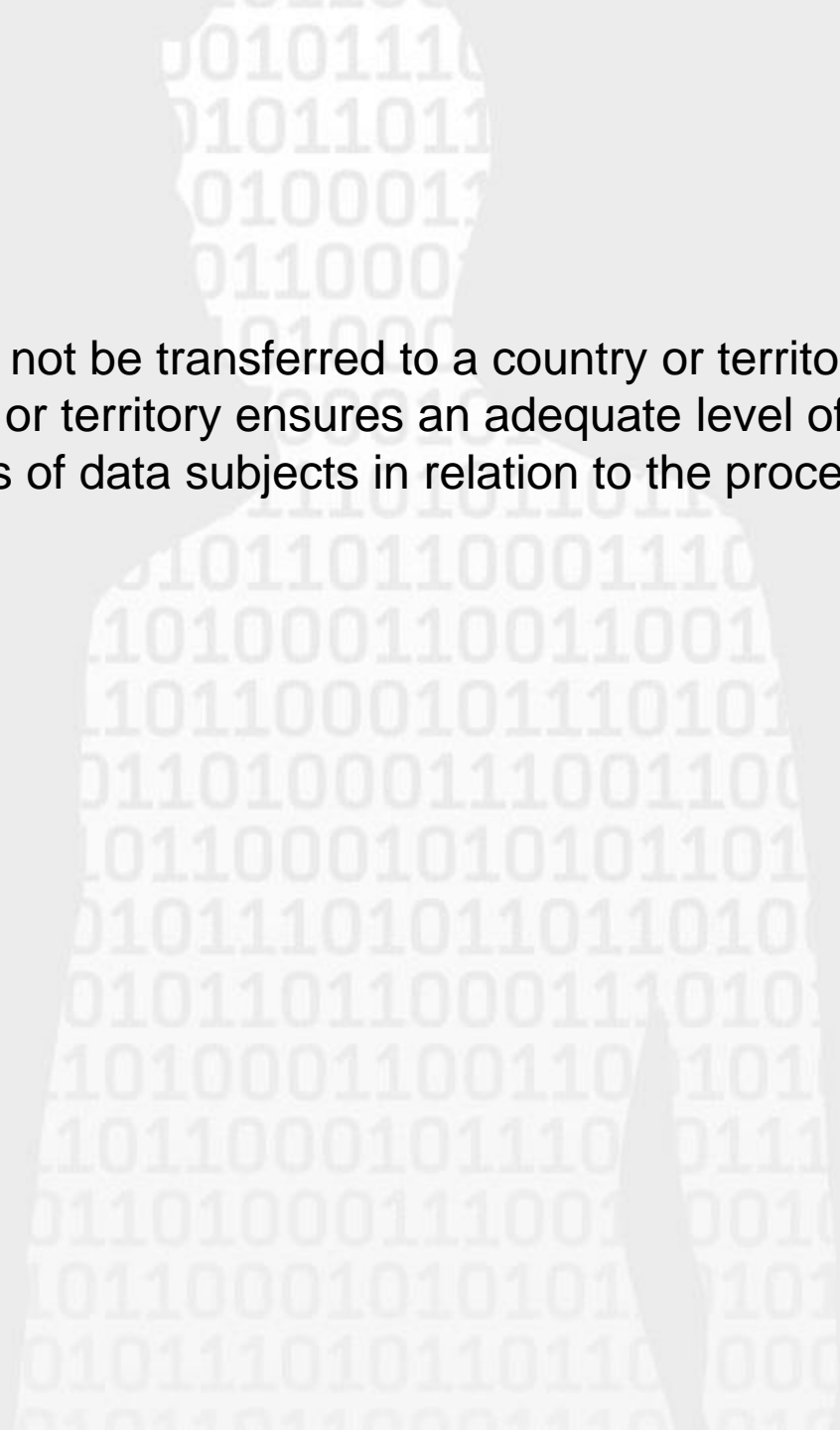
Personal data shall be processed in accordance with the rights of data subjects. The rights of individuals that it refers to are:

- a right of access to a copy of the information comprised in their personal data;
- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to prevent processing for direct marketing;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In practice, it means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. In particular, you will need to:

- design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;
- be clear about who in your organisation is responsible for ensuring information security;
- make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

A faint, light gray silhouette of a person's head and shoulders is centered in the background. The silhouette is filled with a pattern of binary code (0s and 1s) in a lighter shade. The overall background is white, with a red vertical bar on the left and a blue vertical bar on the right.

Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

GDPR

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

GDPR

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

GDPR

While the concept of 'privacy by design' already exists, it has now:

- been given specific recognition,
- and is linked to enforcement

Under the proposed 'privacy by design' requirement, companies will need to design compliant policies, procedures and systems at the outset of any product or process development.

NAME...
AGE... GENDER...
HEIGHT... WEIGHT...
SSN... NET WORTH...
MARITAL STATUS...
PET PEEVES...
WORST FEARS...
SEXUAL FANTASIES...
MEDICAL HISTORY...

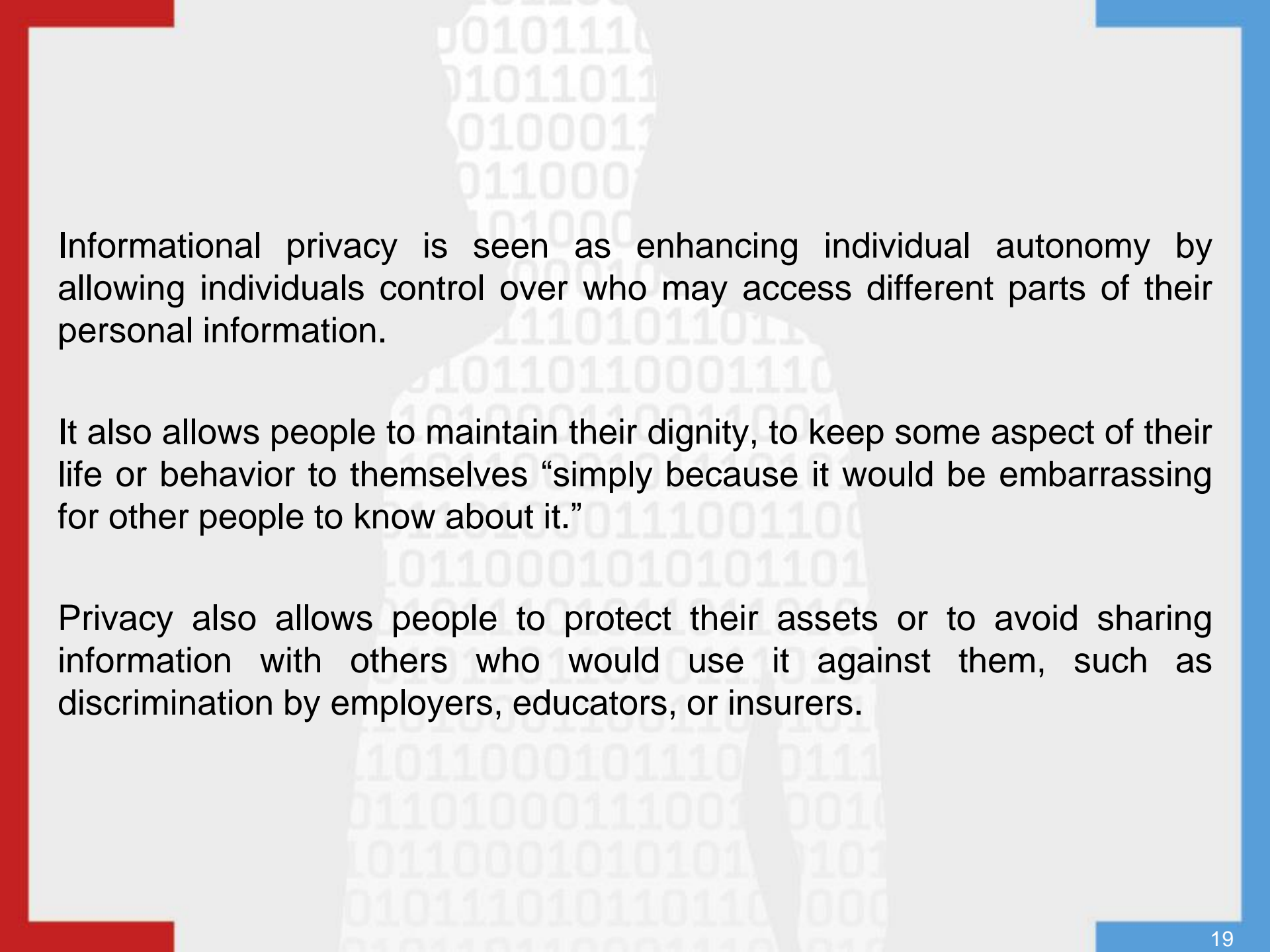
TYPE
TYPE
TYPE
ENTER
ENTER
ENTER

OF COURSE,
I EXPECT
ALL OF THIS
TO REMAIN
STRICTLY
PRIVATE!



Mike Keefe THE DENVER POST 5.26.10

www.caglecartoons.com



Informational privacy is seen as enhancing individual autonomy by allowing individuals control over who may access different parts of their personal information.

It also allows people to maintain their dignity, to keep some aspect of their life or behavior to themselves “simply because it would be embarrassing for other people to know about it.”

Privacy also allows people to protect their assets or to avoid sharing information with others who would use it against them, such as discrimination by employers, educators, or insurers.

Lack of Data Protection (Impacts on individuals)

When personal data is :

- inadequate, insufficient or out of date
- excessive or irrelevant
- kept for too long
- improperly disclosed to others
- used in ways that are unacceptable or unexpected by the person it is about
- used or misused
- not kept securely



Individual at risk of

- physical harm
- threat to emotional wellbeing
- financial loss
- fear of identity theft
- damage to personal relationships
- humiliation/ embarrassment
- harassment
- annoyance

DOGBERT CONSULTS

CUSTOMER DATA IS AN ASSET THAT YOU CAN SELL.



Dilbert.com DilbertCartoonist@gmail.com

IT'S TOTALLY ETHICAL BECAUSE OUR CUSTOMERS WOULD DO THE SAME THING TO US IF THEY COULD.



10-13-10 © 2010 Scott Adams, Inc./Dist. by UFS, Inc.

IN PHASE SOUNDS FAIR. ONE, WE'LL DEHUMANIZE THE ENEMY BY CALLING THEM "DATA."



Lack of Data Protection (Impacts on organizations)

- Damage to an organization's reputation or brand; or pilloried in the public square of opinion;
- Financial losses associated with deterioration in the quality or integrity of personal data;
- Financial losses due to a loss of business or delay in the implementation of a new product or service due to privacy concerns;
- Loss of market share or a drop in stock prices following negative publicity;
- Violation of privacy laws;
- Diminished confidence and trust in the industry
- Fines / Sanctions

■ OWASP Top 10 Privacy Risks Project

(Context: web applications)

- P1 Web Application Vulnerabilities
- P2 Operator-sided Data Leakage
- P3 Insufficient Data Breach Response
- P4 Insufficient Deletion of personal data
- P5 Non-transparent Policies, Terms and Conditions
- P6 Collection of data not required for the primary purpose
- P7 Sharing of data with third party
- P8 Outdated personal data
- P9 Missing or Insufficient Session Expiration
- P10 Insecure Data Transfer

7 principles of PbD

1. ***Proactive*** not ***Reactive***; ***Preventative*** not ***Remedial***
2. **Privacy as the *Default Setting***
3. **Privacy *Embedded* into Design**
4. **Full Functionality – *Positive-Sum*, not *Zero-Sum***
5. **End-to-End Security – *Full Lifecycle Protection***
6. ***Visibility* and *Transparency* – *Keep it Open***
7. ***Respect* for User Privacy – *Keep it User-Centric***



1. Proactive not Reactive; Preventative not Remedial

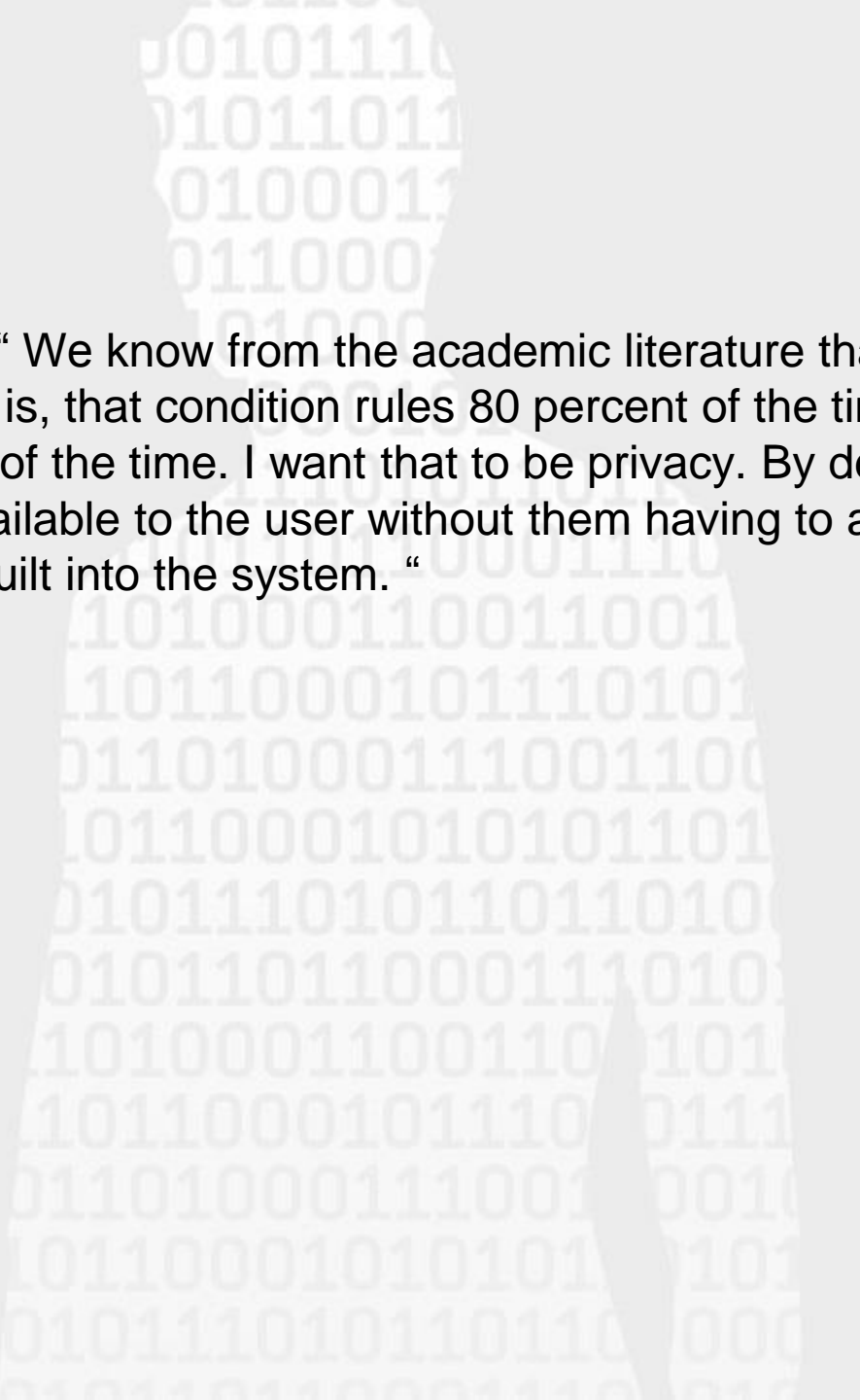
The *Privacy by Design (PbD)* approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. *PbD* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

| Actions | Responsibility |
|---|--|
| <ol style="list-style-type: none"><li data-bbox="287 586 1190 679">1. Affirm senior leadership commitment to a strong, proactive privacy program.<li data-bbox="287 718 1190 858">2. Ensure that concrete actions, not just policies, reflect a commitment to privacy. Monitor through a system of regularly reviewed metrics.<li data-bbox="287 896 1190 1036">3. Develop systematic methods to assess privacy & security risks and to correct any negative impacts, well before they occur.<li data-bbox="287 1075 1190 1215">4. Encourage privacy practices demonstrably shared by diverse user communities and stakeholders, in a culture of continuous improvement. | Leadership/Senior Management e.g. Board of Directors, CEO, CPO, CIO, COO, CSO, Company Owner(s) |

2. Privacy as the *Default Setting*

We can all be certain of one thing – the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, *by default*.

| Actions | Responsibility |
|---|-----------------------------------|
| 1. Adopt as narrow and specific a purpose(s) for data collection as possible – begin with no collection of personally identifiable information – data minimization. | Software Engineers & Developers |
| 2. Minimize the collection of data at the outset to only what is strictly necessary. | Application & Program Owners |
| 3. Limit the use of personal information to the specific purposes for which it was collected. | Line of Business & Process Owners |
| 4. Create technological, policy and procedural barriers to data linkages with personally identifiable information. | Line of Business & Process Owners |

- 
- Ann Cavoukian: “ We know from the academic literature that whatever the default condition is, that condition rules 80 percent of the time. The default rules 80 percent of the time. I want that to be privacy. By default, I mean it's automatically available to the user without them having to ask for it. It's embedded; it's built into the system. “

3. Privacy *Embedded* into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

| Actions | Responsibility |
|--|-----------------------------------|
| 1. Make a Privacy Risk Assessment an integral part of the design stage of any initiative, e.g. when designing the technical architecture of a system, pay particular attention to potential unintended uses of the personal information. | Application & Program Owners |
| 2. Base identity metasegments on the “Laws of Identity,” intended to codify a set of fundamental principles to which universally adopted, sustainable identity architecture must conform. | Line of Business & Process Owners |
| 3. Consider privacy in system development lifecycles and organizational engineering processes. System designers should be encouraged to practice responsible innovation in the field of advanced analytics. | Software Engineers & Developers |
| 4. Embed privacy into regulatory approaches that may take the form of self-regulation, sectoral privacy laws, omnibus privacy legislation and more general legislative frameworks, calling for an approach guided by “flexibility, common sense and pragmatism.” | Regulators |

4. Full Functionality – **Positive-Sum**, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

| Actions | Responsibility |
|---|---|
| 1. Acknowledge that multiple, legitimate business interests must coexist. | Leaders/Senior Management |
| 2. Understand, engage and partner – Practice the 3Cs – communication, consultation and collaboration, to better understand multiple and, at times, divergent interests. | Application & Program Owners Line of Business & Process Owners |
| 3. Pursue innovative solutions and options to achieve multiple functionalities. | Software Engineers & Developers |

- win-win” objectives (privacy, security, business goals)
- do not make trade-offs between security, privacy & functionality: “AND” and not “OR”
- Avoid false dichotomies: ex: privacy vs security

5. End-to-End Security – *Full Lifecycle Protection*

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved – strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.

| Actions | Responsibility |
|--|---|
| 1. Employ encryption by default to mitigate the security concerns associated with the loss, theft or disposal of electronic devices such as laptops, tablets, smartphones, USB memory keys and other external media. The default state of data, if breached, must be “unreadable.” | Software Engineers & Developers Application & Program Owners |
| 2. Deploy encryption correctly and carefully integrate it into devices and workflows in an automatic and seamless manner. | Line of Business & Process Owners |
| 3. Ensure the secure destruction and disposal of personal information at the end of its lifecycle. | |

6. **Visibility and Transparency – Keep it Open**

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

| Actions | Responsibility |
|---|--|
| 1. Make the identity and contact information of the individual(s) responsible for privacy and security available to the public and well known within the organization. | |
| 2. Implement a policy that requires all “public-facing” documents to be written in “plain language” that is easily understood by the individuals whose information is the subject of the policies and procedures. | Leadership/Senior Management Software Engineers |
| 3. Make information about the policies, procedures and controls relating to the management of Personal Information readily available to all individuals. | Application Developers |
| 4. Consider publishing summaries of PIAs, TRAs and independent, third party audit results. | Systems Architect |
| 5. Make available a list of data holdings of Personal Information maintained by your organization. | |
| 6. Make audit tools available so that users can easily determine how their data is stored, protected and used. Users should also be able to determine whether the policies are being properly enforced. | |

© MEX ANDERSON, WWW.ANDERSTOONS.COM



"Before I write my name on the board, I'll need to know how you're planning to use that data."

7. **Respect** for User Privacy – Keep it **User-Centric**

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

| Actions | Responsibility |
|---|---|
| <ol style="list-style-type: none">1. Offer strong privacy defaults.2. Provide appropriate notice.3. Consider user-friendly options:<ol style="list-style-type: none">a. Make user preferences persistent and effective.b. Provide users with access to data about themselves.c. Provide access to the information management practices of the organization. | <p>Leadership/Senior Management</p> <p>Software Engineers & Developers</p> <p>Application & Program Owners</p> <p>Line of Business & Process Owners</p> |

Excerpt from an interview of Ann Cavoukian

(<http://www.bankinfosecurity.com/interviews/privacy-by-redesign-new-concept-i-1171/op-1>)

- Organizations currently exist in a divided environment, working separately instead of together. Engineers for example, in developing systems, don't have a grasp on privacy and aren't expected to. But if the dialogue was open from the beginning, allowing privacy professionals to offer their input, systems could be that much safer from the start, or in the "redesign" phase.
- These are some of the areas where people have to work much more globally across the entire organization. You have to cut through this siloed thinking of we've got this department versus that department. And they don't talk to each other until the product goes to market, and then you've got a data breach and the public goes crazy. This will impact your brand. It will impact your business practices. It will lead to lawsuits and class action lawsuits and it will cost a fortune. Avoid all of that. Avoid the harm by embedding Privacy by Design from the get-go, from the beginning.

Privacy by ReDesign

- To bring privacy into systems that are already developed;
- Just as PbD challenges organizations to think creatively about how all system objectives – including privacy – can be met from the outset, PbRD challenges them to identify and act on opportunities to improve privacy practices going forward by redesigning components of existing systems, based on where they are today;
- **Rethinking, Redesigning, and Reviving** existing systems and their components can involve measures that range from the simple to the complex, and may include policy, operational, technology, or management changes.

Diagram: Implementing *Privacy by ReDesign*

Identify systems
in need of
transformation to
target



Triage potential
targets



| Phase | Rethink | Redesign | Revive |
|-----------------------|---|---|--|
| Objective | Identify business and privacy requirements associated with the target system | Design and develop new controls to meet business and privacy requirements | Rollout redesigned, privacy-enhanced system |
| Key Activities | <p>Confirm/establish business requirements</p> <p>Evaluate existing system privacy controls against <i>PbD</i> Principles</p> <p>Identify deficiencies (gap analysis)</p> <p>Define strategic business objectives, control requirements and initial implementation strategy</p> | <p>Design and build controls that meet business objectives while supporting <i>PbD</i> principles</p> <p>Eliminate earlier existing non-compliant controls</p> <p>Implement new controls</p> <p>Test new controls</p> | <p>Revalidate the redesigned target system against <i>PbD</i> Principles</p> <p>Deploy</p> <p>Confirm successful integration of redesigned target system</p> |
| Outcome | Clear project objectives developed | Redesigned target system with new privacy controls in place | Organizationally-integrated target system aligned with <i>PbD</i> Principles |

Enisa's analysis

- Multilateral security:
 - Whereas system design very often does not or barely consider the end-users' interests, but primarily focuses on owners and operators of the system, multilateral security demands to take into account the privacy and security interests of all parties involved.
 - To realise that, each party should determine the individual interests as well as privacy and security goals and express them.
- Privacy-Enhancing Technologies
- Setup Global Privacy Standards

– The Privacy Principles of ISO/IEC 29100

- specifies a common privacy terminology;
- defines the actors and their roles in processing personally identifiable information (PII);
- describes privacy safeguarding considerations; and
- provides references to known privacy principles for information technology.

– Privacy Protection Goals: *unlinkability*, *transparency*, and *intervenability*

Working with protection goals means to balance the requirements derived from the six protection goals (ICT security and privacy) concerning data, technical and organisational processes. Considerations on lawfulness, fairness and accountability provide guidance for balancing the requirements and deciding on design choices and appropriate safeguards.

PbD in other words

- If an individual does nothing, their privacy still remains intact
- Security and privacy is embedded at every stage in a product
- PbD ensures cradle to grave, secure lifecycle management of information, end-to-end.
- Respect for the choices of individuals
- Users should know the ways their data will be used or shared, and should be able to exercise control
- The security standards, as complex as some of them are, can't cover every possible security scenario, and that's where PbD can step in.

■ “Soft” Privacy

- Reliant principally on trust
- Data subject has to trust honesty and competences of the data controller
- To provide data security and process data with specific purpose and consent
 - => policies
 - => access control
 - => Audit
- user’s consent awareness

- “Hard” Privacy => reduce the need to trust other entities
 - Smaller degree of trust, and establishes concrete protections at, for example, a cryptographic level
 - Unlinkability (key element for data minimization):
 - Aims at separating data and processes
 - Operate processes in such a way that the privacy-relevant data is unlinkable to any other set of privacy-relevant data outside of the domain (or disproportionate efforts)

(hard privacy)

- Intervenability:
 - Possibility for parties involved in any privacy-relevant data processing to interfere with the ongoing or planned data processing
 - Application of corrective measures and counterbalances when necessary

“Intervenability” means the possibility to intervene and encompasses control by the user, but also control by responsible entities over contractors performing data processing on their behalf. Typical examples from the individual’s perspective are giving, denying or withdrawing consent; exercising the rights to access (although this can also be regarded as a transparency functionality), to rectification, to blocking and to erasure of personal data; entering and terminating a contract; installing, de-installing, activating and de-activating a technical component; sending requests or filing complaints concerning privacy-related issues; involving data protection authorities or bringing an action at law.

(hard privacy)

- Transparency
 - To provide an adequate level of clarity of the processes in privacy-relevant data processing so that the collection, processing and use of the information is able to be understood and reconstructed at any time;
 - For all parties: legal, technical and organizational.
- Anonymity, and pseudonymity
- Plausible deniability (vs non-repudiation)
- Undetectability and unobservability: hiding the user's activities
- Confidentiality

High-level keys to success

- Create a culture of privacy in your organization: governance and operations:
 - Challenge: engage the entire ecosystem of an organization
 - A PbD system must facilitate a common understanding between engineers, regulators and managers
- Create “Trust”, confidence and loyalty: Trust is a key factor for economic growth
- PbD = Key argument for selling innovative technology

Some mistakes to avoid

- Think about including privacy and data protection requirements at the end of the project
- Focus only on legal compliance
- To assess impacts of risks only on your organization's and not on the data subjects
- Function creep as Feature: a widening of the data processing beyond the original purpose or context
 - ⇒ Economist are trained to exploit available data for multi-purpose usage
 - ⇒ Data are taken out of the original context which can lead to wrong conclusion when interpreting the data

Privacy enhancing technologies

- a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system
- incorporating legal principles into technical specifications (ex: data minimization)
- The choice of PET techniques depends on the level of security needed to match the level of risks represented by the personal data.

Privacy enhancing technologies (Privacy preserving PETS)

- Usage of cryptography for:
 - Data storage
 - Authorization
 - Data access and data disclosure (at an application level, rather than at a DB level)
 - Data transport (network and other means)

- Biometrics: an opportunity and threat at the same time
- Creation of audit trails
- Usage of pseudo-identities: TTP
- Tracking protection lists in Internet Explorer

Privacy enhancing technologies (Privacy preserving PETS)

- Enhanced privacy ID (EPID) is a digital signature algorithm supporting anonymity. Unlike traditional digital signature algorithms (e.g., PKI), in which each entity has a unique public verification key and a unique private signature key, EPID provides a common group public verification key associated with many of unique private signature keys.

EPID was created so that a device could prove to an external party what kind of device it is (and optionally what software is running on the device) without needing to also reveal exact identity, i.e., to prove you are an authentic member of a group without revealing which member.

Transparency enhancing technologies (Privacy friendly PETS)

- A category of tools that supports:
 - The right to be informed
 - The right for the subject to know what happens to his personal data

Examples:

- Privacy icons
- Dashboard functionality on a website
- Browser Addons: Privacy Bird, Collusion, Web Of Trust, ...
- Guichet.lu: logs of access performed by administration on your data from the RNPP.

=> To promote trust of the users and willingness to use a particular online service

But not only technologies

- An unexpected example:
 - Buying your medicines in a pharmacy
 - Privacy risk: you might not want to share with all the other waiting customers information about your disease.
 - Potential solution: the shop could put some information on the desk informing the customer that he can request for a discussion in an area that provides privacy

=> It is also Privacy by Design

Bibliography

- Privacy by Design ...take the challenge – Ann Cavoukian
- Privacy by Design – Curriculum 2.0: the fundamentals (www.privacybydesign.ca)
- Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices – Ann Cavoukian (2012)
- Why Privacy by Design is the next crucial step for privacy protection (by Simon Davies – November 2010)
- A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements (Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, Wouter Joosen – KU Leuven)
- The control over personal data: True remedy or Fairy tale? (Christophe Lazaro, Daniel L Métayer, Research report no 8681, Inria, ISSN 0249-6399)
- Transparency enhancing tools (TETs): an overview (Milena Janic, Jan Pieter Wijbenga, Thijs Veugen – Delft University of technology, The Netherlands)
- Handbook of Privacy and Privacy enhancing technologies (G.W. van Blarckom, J.J. Borking, J.G.E. Oik – PISA)
- Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals (Marit Hansen, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)
- Privacy and Data Protection by Design – from policy to engineering (Enisa)

Bibliography

- OWASP TOP 10 Privacy risk Project (https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project)
- <http://privacylawblog.fieldfisher.com/category/privacy-by-design>
- Providing consumer privacy in an era of rapid change (<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>)
- Privacy by ReDesign: A practical framework for implementation (<http://securityandprivacy.ca/download/new/Informatica-PbRD-framework.pdf>)
- Privacy by ReDesign: Building a better legacy (<https://www.ipc.on.ca/images/Resources/PbRD.pdf>)
- Wikipedia – Privacy Enhancing Technologies (https://en.wikipedia.org/wiki/Privacy-enhancing_technologies)

“Building in privacy might not to be cheap, but just cheaper than building in no privacy”

Thank you for your attention.



Alain Herrmann
INFORMATIQUE ET NOUVELLES TECHNOLOGIES

Commission nationale pour la protection des données
1, avenue du Rock'n'Roll | L-4361 Esch-sur-Alzette
Tél. : (+352) 26 10 60 51 | Fax : (+352) 26 10 60 29
alain.herrmann@cnpd.lu | www.cnpd.lu