Privacy Cookbook for Business Processes

As resource for IPEN

(Internet Privacy Engineering Network)

– draft – V0.0002 – TO BE DISCUSSED -

Nightly build – 16.10.2014

Begun by Markus Alexander Grete – feel free to participate !!!

Company Mail address: [Markus.Grete@gretEDV.de](mailto:Markus.Grete@gretEDV.de)

University Mail address: [grete@l3s.de](mailto:grete@l3s.de)

# Motivation

If you are in Business Process Modelling (BPM), you need to care about the privacy topics.   
Let’s start with the basics.

## The 7 basic principles of privacy

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as 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

## Basic concepts of privacy

* the right to be forgotten
* the minimum acquisition of data
* the processing by consent
* anonymity
* purpose-specification
* […] help me to continue!

## Into

As we consider privacy in IT systems, we have to deal with the basic principles of privacy. As to (3.) we have to embed privacy into design. As to (2) by default. That means that we have to consider privacy from the first step on.

Very often in software development in Year 2014 the software development process begins with an analysis of what is needed, an analysis of the Business Process (BP) the software has to support.

So we are starting top-down here.

## Basic real-world problems making privacy more difficult

(Reasons for the need to preserve data)

* Requirements of completeness for audits
* Requirements for preparation against legal trails
* […] help me to continue!

## The real world outside

You can introduce privacy into business process modelling once at each project, or – if you are a consultant – once at each customer. And you can install a separate privacy guiding process in addition to the casual data protection guidelines or compliance guidelines almost every bigger company has. If you enter a fresh startup, you should try to install a privacy guiding process as data protection guideline, combining everything.

But to be honest, to me this is the boring part of the work and should be automated via standardized documentation (cookbooks) and tools. That’s why I suppose we need a cookbook for that.

The interesting part is to analyze the existing (sometimes older and “established”) business processes and data dictionaries, the business requirements and the current legal prerequisites. Moreover you have to look at the Databases and flat files, the Queues and Enterprise Service Buses and whether all of them are covered in the BP documentation. And – not for last – the Online- and Offline applications and their BP coverage.

Consider: If a business process (BP) is running untouched for more than 5 years, it will most probably not be up to date in all respects. And each time you pick up a BP you have to ask all the experts and sometimes use a lot of time to get all things done.

# Borderlines

## Topic borderline

In this cookbook we do not want to care much about the engineering or solely cryptographic perspective of privacy within applications. That will be topic of another cookbook. Nevertheless we will take every hint we get and assimilate it as good as we can.

## Opinion borderline

Some of us have to make money out of the privacy business, my company too. So if I consider a document in the literature index to be more a “commercial” document - that does not mean I do not like it. We will have documents from “hactivisim”, “science”, “engineering”, “commerce” and “legal” sources. That is what IPEN was built for, to combine those ideas. I will not go out and evaluate one of them to be bad or good from my point of view as I have very good friends in each of the privacy flavors.

## Cost and security borderline

I don’t know why, but I learned that companies usually do not want to show that they care about security or privacy, and want to keep their privacy enforcing projects secret. They do not even want the company name on any scientific slide about the “next generation” things we installed.

The only thing I can estimate about that is that a company’s customer would think: “Hey, they have to improve their privacy ruleset, there must be something wrong about it!”. The opposite is correct. [Kaizen](http://en.wikipedia.org/wiki/Kaizen) rules.

But – therefore – I cannot supply customer’s project documentation and can only start from now on to tell the customers that everything we do could but needn’t lead to a passage in the cookbook. If you have something you could pseudonymize[[1]](#footnote-1) and supply, you’re welcome.

Contents

[Motivation 2](#_Toc401217819)

[The 7 basic principles of privacy 2](#_Toc401217820)

[Basic concepts of privacy 2](#_Toc401217821)

[Into 2](#_Toc401217822)

[Basic real-world problems making privacy more difficult 2](#_Toc401217823)

[The real world outside 2](#_Toc401217824)

[Borderlines 3](#_Toc401217825)

[Topic borderline 3](#_Toc401217826)

[Opinion borderline 3](#_Toc401217827)

[Cost and security borderline 3](#_Toc401217828)

[Main document 5](#_Toc401217829)

[Lifecycles 5](#_Toc401217830)

[Customer Lifecycle 5](#_Toc401217831)

[Business Process Lifecycle 5](#_Toc401217832)

[Data retention in common 5](#_Toc401217833)

[Ideas 5](#_Toc401217834)

[Toolsets 5](#_Toc401217835)

[Literature 6](#_Toc401217836)

[Companies and Projects 9](#_Toc401217837)

[Persons 10](#_Toc401217838)

[Glossary 11](#_Toc401217839)

## Main document

- STARTING -

## Lifecycles

### Customer Lifecycle

If the data of a customer is no longer needed, it can and should be deleted. If a separate part of customer data is no longer needed, it should be disposed.

### Business Process Lifecycle

If a Business Process is finished, the data which was collected for this business process only should be deleted. The speed of this removal depends mostly on “Basic real-world problems making privacy more difficult”.

### Data retention in common

[…] help me to continue!

## Ideas

Installation of “next generation” access control mechanism as Attribute Based Access Control.

Installation of “Power to the person described by the data” (sometimes “more power to the user”, which would only sound correct in systems where the user is entering the data on his own).

## Toolsets

If you can support tables etc. which can be used with e.g. Open Office or similar, please support.

If you are from a software vendor for BPM, please support.

# Literature

Danger: The comment “Useable here for\*” in the tables below is very from my point of view and towards what I think on my own. Please feel free to get me informed, when I am wrong from your point of view.

|  |  |
| --- | --- |
| Title | Attribute Based Access Control |
| Information supplied by | MG |
| Useable here for\* | Restricting rights with state-of-the-art Access Systems |
| Download-Page | <http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf> |
| Further Information | For further information: Prof. Ravi Sandhu |
| Added | 16.10.2014 |

|  |  |
| --- | --- |
| Title | Android Application Secure Design/Secure Coding Guidebook |
| Information supplied by | JSSEC.ORG / via FD |
| Useable here for\* | Heading towards Round-Trip engineering privacy |
| Download-Page | <http://www.jssec.org/English> |
| Further Information | Seems to [MAG] as a technical and technological Guidebook |
| Added | 04.10.2014 |

|  |  |
| --- | --- |
| Title | Enable secure product delivery |
| Information supplied by | FD |
| Useable here for\* | Thinking about basic processes as already established to secure coding |
| Download-Page | <http://www8.hp.com/h20195/v2/GetPDF.aspx/4AA5-3485ENW.pdf> |
| Further Information |  |
| Added | 04.10.2014 |

|  |  |
| --- | --- |
| Title | Engineering privacy requirements |
| Information supplied by | JMdA |
| Useable here for\* | More for the engineering cookbook |
| Download-Page | The document is available in IEEE Xplore Digital Library at <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6890523> |
| Further Information | Martin, Y.S., Del Álamo, J.M., Yelmo, J.C., Privacy Requirements Engineering: Valuable Lessons from Another Realm, In 1st International Workshop on Evolving Security and Privacy Requirements Engineering - ESPRE2014, pp. 19-24, Karlskrona (Sweden), 25 Aug 2014. doi: 10.1109/ESPRE.2014.6890523 |
| Added | 04.10.2014 |

|  |  |
| --- | --- |
| Title | Linking security with Economics |
| Information supplied by | SJE |
| Useable here for\* | Finding the business and economic value of privacy |
| Download-Page | <https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Stephan.pdf> |
| Further Information | SJE supplied more links which seem not very important for this document because they are more technological related. Just picked one which could help to understand his point of view:  <http://blog.privacytrust.eu/public/Slides/au_conf670306_engberg_en.pdf> |
| Added | 04.10.2014 |
| Title | Model-driven security |
| Information supplied by | UL |
| Useable here for\* | Evaluation of Model driven security |
| Download-Page | http://en.wikipedia.org/wiki/Model-driven\_security |
| Further Information |  |
| Added | 16.10.2014 |

|  |  |
| --- | --- |
| Title | New Digital Security Models |
| Information supplied by | SJE |
| Useable here for\* | Telco / ITK privacy issues |
| Download-Page | <http://blog.privacytrust.eu/public/Reports/NewDigitalSecurityModels.pdf> |
| Further Information |  |
| Added | 04.10.2014 |

|  |  |
| --- | --- |
| Title | Privacy Engineering – A dataflow and ontological approach |
| Information supplied by | FS |
| Useable here for\* | “it is about applying a structured approach to classification and modelling at data, storage, process, user, and environmental level, illustrated with a few use-cases  It has a proposed (or "sample") vocabulary/taxonomy with the aim of engendering PbD from requirements gathering through to end-of-life, and a means to communicate in the organisation, engineering and legal teams. So its not a "cookbook" in my mind, and is one approach to PbD in the engineering lifecycle. As an example of the depth that data modelling for privacy can go to it is good, I think, but it may not be suitable for all organisations.” as to UXOC  “I’ve got a copy of the book – have read the initial chapters.  I really like the modelling approach he takes – which encourages drilling down from high level data flows that anyone can understand, to the technical levels where privacy controls can actually get built in.” as to RB |
| Download-Page | <http://www.privacyengineeringbook.net> (only overview, Amazon book) |
| Further Information | Book by Ian Oliver |
| Added | 16.10.2014 |

|  |  |
| --- | --- |
| Title | “Salt” spelled: NaCl |
| Information supplied by | CvL |
| Useable here for\* | More for the engineering cookbook – About a network comm. library |
| Download-Page | <http://cdn.media.ccc.de/congress/2013/workshops/30c3-WS-en-YBTI_OS-Bernstein_Lange_Schwabe-NaCl_and_TweetNaCl.webm> |
| Further Information | <http://cdn.media.ccc.de/congress/2013/workshops/30c3-WS-en-YBTI_OS-Jon_Solworth-Ethos_Operating_System.webm> |
| Added | 04.10.2014 |

# Companies and Projects

| **Homepage** | **Suggested by** | **Info** |
| --- | --- | --- |
| <http://governor.co.uk> | [MAG] | <<< PLEASE SUPPLY INFORMATION >>> |
| <http://objectsecurity.com/en-home.html> | [MAG] | <<< PLEASE SUPPLY INFORMATION >>> |
| <http://pripareproject.eu/> | [CJ] | “PReparing Industry to Privacy-by-design by supporting its Application in Research”  Seems a good attempt. Interested ones should read.  <http://pripareproject.eu/wp-content/uploads/2014/06/PRIPARE-Position-Paper-v1-WP1.pdf> |
| <https://cryptech.is/> | [EJ] | They are doing crypto stuff for secured communication. Seem to have some guidelines for HW-design and -evaluation. |

# Persons

If you want **your Name added**, just send me an email from the email account I have to add.   
If you want **your Name deleted** because you do not it in a book which is not 100% flavored as you like, or you do not want the information in display, please send me an email.

**But please understand: We cannot keep the discussion going on without knowing who has which special knowledge or opinion. Just as community we can correlate all the information.**

| **Name** | **“Real” Name** | **Task for IPEN** |
| --- | --- | --- |
| [AB] | Aral Balkan | => Engineers cookbook  Nice project |
| [CJ] | Christophe Jouvray | Supplies project information |
| [CvL] | Carlo von Lynx | Supplies Info about end-to-end encryption, is IPEN lead for mobile solutions |
| [EJ] | Erik JOSEFSSON | Supplies company Information |
| [FD] | Frank Dawson | Supplies literature |
| [FS] | Florian Stahl | Supplies information. OWASP might supply “counter-measures” (?) |
| [JMdA] | José M. del Álamo | Supplies research documentation |
| [MAG] | Markus Alexander Grete | Cook at the the Privacy Cookbook for Business Process |
| [MON] | Mike O'Neill | => Engineers cookbook |
| [RB] | Richard Beaumont | Supplies information, see governor.co.uk for company information |
| [SJE] | Stephan J. Engberg | Supplies slides and PDF |
| UL | Ulrich Lang | Supplies information about MD-Security |
| UXOC | Ultan X. O’Carroll | Data protection of Ireland, Supplies information and knowledge |

# Glossary

| **Short** | **Element** | **Abstract** |
| --- | --- | --- |
| ABAC | Attribute Based Access Control | Idea: Prof. Ravi Sandhu  @see “Literature” above / „Attribute Based Access Control“ |
| BDSG | Bundesdatenschutzgesetz | German federal law for data protection |
| BP | Business Process | Please refer to: <http://en.wikipedia.org/wiki/Business_process> |
| BPM | Business Process Modelling | Constructing BP’s |
| PbD | Privacy by Design | Please refer to:  <http://en.wikipedia.org/wiki/Privacy_by_Design> |

1. Sorry, in Germany we must make a difference between anonymized and pseudonymized as to “BDSG” law. [↑](#footnote-ref-1)