Document 2.1.4 - 7

GUIDELINES ON PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENT

Component 2

Activity 2.1.4 - 4

Draft version - November 2011

The content of this report is the sole responsibility of Human Dynamics and can in no way be taken to reflect the views of the European Union

Table of Contents

I. INTRODUCTION

These Guidelines set the basic principles and guidelines for assuring that the future of privacy will be ensured as organisation's mode of operation. It means that not only regulatory framework will protect privacy assurance but new operation measures of producers who will take privacy into consideration from the beginning of development of the product. The concept "Privacy by Design" is the philosophy proposed by Mrs Ann Cavoukian, Ontario Information and Privacy Commissioner" in the 90's year of last century. The concept is based on the idea of PET (Privacy Enhancing Technology) and well known PIA (Privacy Impact Assessment). The Privacy by Design is characterized by proactive approach; it anticipates and protects privacy against negative and invasive effects of new products and technologies before they happen. Important aspect of Privacy by Design is **preventive** effect.

Purpose/aim of the document

This document's aim is to demonstrate that protection of privacy must cover not only reactive measures but also **preventive** ones. The privacy by design regime is proper for public authorities as well as private organisations to ensure that protection of privacy will accompany all phases of processing of personal data in information systems. The document presents the core principles of both Privacy Impact Assessment (PIA) as well as Privacy by Design approaches. To be effective, both PIA and Privacy by Design need to be an integral part of the planning process (rather than an afterthought). The purpose of both approaches is to identify the potential effects that the proposed processes may have upon privacy of persons and also examine how any detrimental effects on privacy might be lessened.

As the author recalls, the Privacy by Design encompasses many elements in practice:

- Recognition that privacy interests and concerns must be addressed,
- Application of basic principles expressing universal spheres of privacy protect,
- Early mitigation of privacy concerns when developing information technology and systems, across the entire information life cycle,
- Need for qualified privacy leadership and/or professional input, and
- Adoption and integration of privacy-enhancing technologies (PETs). [1]

When talking about Privacy by Design we must not forget the Privacy Impact Assessment (PIA) process. See the aim of PIA and compare it with Privacy by Design: PIA aim is to identify the potential privacy risks of new or redesigned programs, systems or products. We can see that both processes focus on preventive aspects of new products, not to systems or products already applied.

[1] Ann Cavoukian – Privacy by Design (see References)

The purpose of these Guidelines is to provide a comprehensive framework on the role, the scope and conduct of Privacy Impact Assessment. The Guidelines provide practical advices how the PIA will be organised and what are the main parts of the process. Key goal of the PIA is to effectively communicate and manage privacy risks not addressed through other control mechanisms (e.g. privacy compliance audits). Privacy compliance audit is carried out on existing system to ensure its conformity with internal rules and legal requirements in relation to privacy and data protection. On the other side, PIA focuses on understanding a proposed system (or the effects of proposed changes to an existing system). PIA aim is to identify and reduce future adverse impacts as well as to inform project managers about whether a project should proceed and in what forms. However, it must be known that distinction between both techniques is not absolute – there may be helpful and useful inter-relationship between.

The PIA ensures that privacy principles lay down by the Law on protection of personal data (LPDP) and other data protection legislation are considered and keep to throughout the lifecycle of a new program, information system, service or process.

It must be noted that these Guidelines do not focus on issues relating to privacy and data protection compliance audit (internal or external).

TECHNICAL BACKGROUND

The PIA process can be used by any institution handling personal information. The procedure is especially suited to medium and large companies as well as to government institutions. The Privacy Impact Assessment (PIA) process consists of following steps:

Step 1: Project Initiation

If the initiative is at the early concept or design stage and detailed information is unknown, then the institution should consider conducting a **Preliminary Privacy Impact Assessment (Preliminary PIA)**. If this Preliminary PIA shows a privacy risks then the institution decides on necessity to conduct a full PIA process.

Step 2: Data Flow Analysis

The purpose of this step is to analyse the personal data flows within information system of the organisation. It involves a description and analysis of the business processes, architecture and detailed data flows.

Step 3: Privacy Analysis

The privacy analysis examines the data flows in the context of applicable privacy and data protection policies and legislation. A special questionnaire helps to collect relevant information on personal data flows. The Questionnaire is used as a checklist that facilitates the identification of major privacy and data protection risks or vulnerabilities associated with the proposal.

Step 4: Privacy Impact Analysis Report

This is the final and most critical component of the privacy impact assessment process. This phase analyses and processes the outputs from previous steps and suggests next procedures and a scope of PIA. This phase documented evaluation of the privacy and data protection risks and associates the implications of those risks along with a discussion of strategy for elimination or mitigation of these risks.

II. APPLICATION OF THESE GUIDELINES

What are Privacy Impact Assessments?

PIA is a tool for systematic analysis of privacy and data protection issues related to information system of an organisation. PIA provides warning information which can be used for adoption of correctional measures. Privacy (and Data Protection) Impact Assessment may play role of "early warning system" for organisations. It is effective instrument for management to be informed about all risks and help them adopt relevant decisions to avoid privacy disasters.

Who should use Privacy Impact Assessments?

PIA is a process that can be used by any institution handling personal data, regardless it is data controller, data processor or data user. This document is dedicated to them with the aim to help them find out possible mistakes and problems which may affect compliance with privacy and data protection. The use of PIA demonstrates that organisation pays serious care to processing of personal information.

Such a demonstration contributes to increasing of credibility and reputation of a organisation and offers better competitive advantage between their rivals.

The person/s that undertake an assessment and complete a privacy impact assessment report have to have a variety of skills. The PIA assessment shall be made by a group of persons who have sound analytical and writing skills and enough of experience in protection of privacy. The person/s need to be familiar with information privacy, data protection legislation, security approaches and analysis of possible risks to privacy of individuals.

The person/s undertaking the Privacy Impact Assessment process and writing outcome report need to be experienced in following areas in particular:

- the company policy development, including business-specific policy experience, broad strategy policy of the institution and its planning for future;

- knowledge of operational programme and business design of the company. The expert shall be able to examine proposals for the operational flow of the business, analyse the feasibility, practicality, and efficiency of relevant aspects of the project or the company's information system and to respond the privacy risks.

EXAMPLE OF QUESTIONS IN PIA PROCESS

Before starting the PIA process the institution shall set up a list of questions which will be dealt with. Of course, the scope of the questions depends on the line of business of the institution. There are two forms of questions – first the questions accompanied which checkboxes: YES/NO/In progress/Not available. The second ones are question where answer is in provided in free text. An example of this questionnaire is elaborated further in the second part of this Guideline - **How to perform a Data Protection and Privacy Impact Assessment?**

PRIVACY IMPACT ASSESSMENT (PIA) REPORT

First key output of PIA is the Report. There are several common elements that each PIA Report needs to cover. One typical table of content of PIA Report is the following:

- **Introduction and overview**
- **Executive summary**

- **Description of the project**
- **Data (information) flow analysis**
- **The privacy analysis: (collecting and obtaining information; use, processing, disclosure, disposition and retention of information)**
- **Privacy risk assessment**
- **Privacy enhancing responses**
- **Compliance mechanisms**
- **Conclusions**

A brief description of the elements of the Report:

Introduction and overview – this part of the Report describes and summarises the objectives the report, scope of PIA, reference documentation, participants (a list of experts attended the PIA), list of any legislation or policies that may apply to the privacy requirements that affect the project proposal). The report needs to be written in such a way that it will easily be understood by non-technical people, managers, decision-makers and so like.

Executive summary – it is the appropriate way to communicate the results of PIA with the public.

Description of the project – contains narrative description of the project proposal, including objectives, rationale, clients, approach, programs, and also involved partners.

Data flow analysis – completes a data (information) flow table to follow each data element or cluster (i.e. group of elements that can be tracked as a unit) from data collection through use and disclosure.

Privacy analysis – consists of yes/no responses to a series of questions along with a comments section. The analysis also covers the explanation how a particular requirement is met or why it is not met. For this part of PIA it is necessary to set up questionnaires with questions derived from universal privacy requirements as well as requirements of the Law on Personal Data Protection (LPDP) and/or other legal documents. The report should not limit itself to compliance issues and should discuss and analyse the proposal with respect to the potential advantages and risks in information privacy terms and identify best practice when possible.

Collecting and obtaining information – describes personal data that is collected and indicates the source of each item of data. All circumstances and means of collecting should be explained, purposed for which data is collected, etc.

Use, disclosure, process, and retention of information – all aspects should be described carefully.

Privacy risk assessment – all risks of the project must be summarised and assessed. Risks to privacy can arise in many circumstances – excessive collection of data, using intrusive means of collection, obtaining sensitive data in unexpected circumstances, unexpected or unwelcome use or disclosure of personal data, retention data for unduly long period, all these put privacy at risk. The PIA report should to sort out which risks are serious and which are trivial. The report should identify the avoidable risks and suggest cost-effective measures to reduce them to an appropriate level.

Privacy enhancing responses – suitable responses can range from doing nothing, through to abandoning the project altogether. A range of privacy enhancing responses may be appropriate to the identified risks. One set of responses involves security safeguards appropriate to the sensitivity of data. The Law on PDP requires that all reasonable steps to be taken to ensure that personal data is protected against loss, unauthorized access, use, modification or disclosure, or other misuse. The security measures should respond to the risks as identified in the privacy impact report. PIA does not seek merely to identify the strongest information security. It seeks to identify the most appropriate level of security. The report should provide support and recommendation on security safeguards.

Compliance mechanism – A PIA should consider how the privacy risks of the project will continue to be appropriately controlled into the future. For example, an effective Privacy Officer or privacy team may be appointed.

Conclusions – it may convey the following information – description of the proposal, overview of relevant privacy requirements incl. applicable law, overview of specific privacy risks, etc.

III. PRIVACY BY DESIGN (PBD)

What is Privacy by design?

Privacy by Design (*PbD*) is a concept introduced in the 1990s by Ontario's Information and Privacy Commissioner Dr. Ann Cavoukian. The philosophy of *PbD* is embedding privacy from the outset into the design specifications of information technologies, accountable business processes, physical spaces, and networked infrastructures. Privacy by Design is a proactive approach to protecting the privacy of individuals. Many other privacy protection concepts are associated with reactive approach frameworks which cover reactions for privacy breaches occurred in information technology application. Reactive approach, based mostly on legal compliance is not sufficient enough in the era of rapid pace of technological progress and changes. The *PbD* therefore is called as "the new generation of privacy protection".

While the PIA concept focuses on an organisation's compliance with legislative and regulatory requirements, the *PbD* concept assumes a holistic approach by transforming how an organisation manages the privacy from policy and compliance to an organisation-wide business issue and strategy. The *PbD* approach adopts holistic approach to privacy by:

- ✓ ensuring privacy protection is embedded into information technology, business processes, physical spaces and networked infrastructures from the outset; and
- ✓ encouraging organisation to adopt the *PbD* Principles into all aspects of their operations wherever and whenever personal information is collected, used, disclosed, retained, transferred, and/or disposed.

The *PbD* framework discusses the application of the seven *PbD* Principles in three areas:

1) Information technology;
2) Accountable business processes, and
3) Physical design and networked infrastructure.

The organization's approach to privacy protection can be assessed against the seven *PbD* Principles to establish its overall privacy posture. The seven *PbD* Principles are[2]:

1. **Proactive** not Reactive—Preventative not Remedial.

(Prevention of privacy breaches from occurring)

2. Privacy as the **Default Setting.**

(No action is required on the part of individuals to protect their privacy—privacy is built into the Application by default)

3. Privacy **Embedded** into Design.

(The privacy becomes an essential component of the core functionality being delivered)

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

(*PbD* avoids the pretence of false dichotomies, such as privacy vs. security. Privacy does not gain or lose at the expense of functionality and security)

5. End-to-End Security—**Full Life Cycle Protection.**

(*PbD is* embedded into the Application prior to the collection of any personal information, extends throughout the entire life cycle of the personal information involved)

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

(An organization's Applications must conform to its stated privacy and security practices. These practices are subject to independent verification, and are made visible and transparent to all)

[2] Cavoukian, Ann, PhD., Information & Privacy Commissioner, Ontario Canada, Privacy by Design *The 7 Foundational Principles Implementation and Mapping of Fair Information Practices* (Originally published: May 2010, Revised January: 2011), at http://www.ipc.on.ca/images/Resources/pbd-implement-7found-principles.pdf

7. Respect for User Privacy—**Keep it Individual and User-Centric.**

(The privacy interests of the individual are paramount and kept uppermost in mind and practice through the implementation of, and compliance with, privacy practices and security protections that are embedded into an organization's information technology, business processes, physical spaces and networked infrastructure).

Privacy by Design framework and the Privacy Impact Assessment concept are complementary models for incorporating privacy of individuals into design, development and deployment of systems deals with personal information. The close relation between both concepts demonstrates also frequently uses title for PbD – "Privacy by Design Privacy Impact Assessment". The *PbD* PIA does not necessarily replace a traditional 'compliance-based' Privacy Impact Assessment (PIA), or other methodologies an organization may use for conducting a privacy and data protection risk analysis. Rather, it augments such work. The *PbD* framework provides an opportunity for an organization to make certain that all necessary privacy and security controls are in place to ensure that an individual's information is adequately protected throughout its life cycle by applying the holistic approach of the *PbD* Principles. The *PbD* PIA can thus serve as a building block for the organization's information governance and risk management program.

IV. THE DIRECTORATE FOR PERSONAL DATA PROTECTION (DPDP)

For the purpose of supervising the lawfulness of the undertaken activities while processing and protecting personal data, the Directorate for personal data protection (DPDP) is established as an independent state body. Inspection supervision over the implementation of the LPDP and the regulations adopted on the basis of this Law is performed by the DPDP inspectors for personal data protection.

Because a company's system gathers and processes personal data about individuals, such a system falls under data protection legal regime as stipulates the Law on Personal Data Protection. The DPDP is competent to supervise the system carried out by or on behalf of the institutions and companies.

The DPDP shall also be consulted in any specific cases, for instance when a system processes sensitive data, if the system purpose is monitoring individuals, etc.

Besides performing inspection supervision the DPDP also provides assistance for personal data processing to all interested persons. This means that data controllers, data processors or any private or public body can consult the DPDP if they face any difficulties or if they simply want consultation on regarding better and more professional performing of the PIA.

For finding more information on data protection issues the data controllers and processor can simply visit the web page of the DPDP www.privacy.mk or www.dzlp.mk. The web page contains useful information on protection of privacy as well as links on how to contact the DPDP.

V. HOW TO PERFORM A DATA PROTECTION AND PRIVACY IMPACT ASSESMENT?

The aim of this part of the Guideline is to provide concrete guidance to data controllers how to actually perform a Data Protection and Privacy Impact Assessment (hereinafter: DPIA), explaining **who**, **why** and **how** should a DPIA be conducted as well as to provide concrete real-life examples.

Why are DPIAs useful?

Data protection authorities have in their day-to-day practice, often been confronted by a situation where irregularities and infringements have been established during inspection procedures. A great many of these would not have occurred if the liable person (the controller or the processor of personal data), had timely **conducted a DPIA before implementing a certain project** or before using a certain technology. In such a way the DPIA would have decreased the risk of an occurrence of any such illegality or eliminated the risk in its entirety.

The relevance and the efficiency of the PIA increases with the scope and intensity of the personal data involved in a particular project, whereby a 'project' may be understood as any of the following:

- Change of legislation
- Introduction, connection or development of new information solutions
- Practical application of a certain technology
- Expansion of the initial purpose of personal data processing, or the manner of processing (e.g. data transfer)
- Some other important change in the business environment which may exert a significant impact on personal data protection.

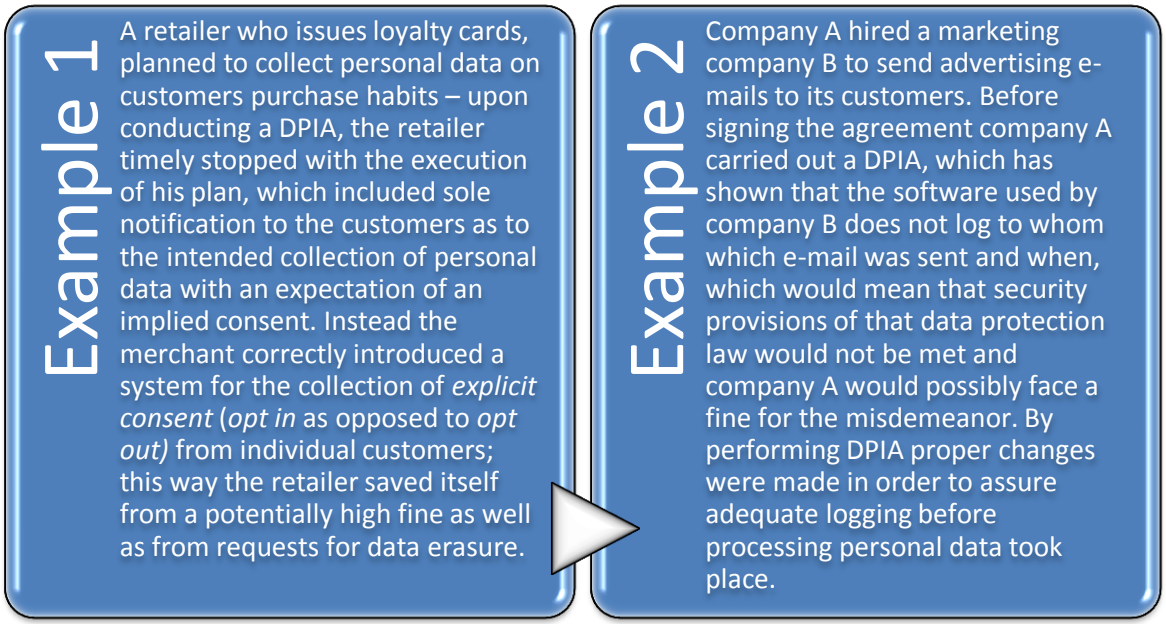
On many occasions it is possible to fulfill a project's objectives in a manner which does not require processing of personal data, or requires processing of a smaller amount of personal data. By taking into consideration the concept of Privacy by Design it is easier to achieve compliance with fundamental legal principles and requirements. Sentences such as: '*Let's collect this data too – we might find it useful!*', or '*Best not to permanently erase this, you never know when we might need it*.' and '*The technology enables us to collect and process all this data, so we might as well take advantage of it*.' are all **classic mistakes** in basic thinking, which later leads to problems in attempting to achieve compliance with data protection law.

By conducting the DPIA, and by considering Privacy by Design, one can also **avoid the so-called "function creep" phenomenon**, where data is primarily collected for a certain purpose and then, after a time, it is also used for other purposes, by other erstwhile unknown processors and users.

The DPIA guidelines place emphasis upon simplicity, practicality, rationality, with the aim of avoiding unlawful data processing and by no means through the creation of administrative barriers in terms of a complicated formal application of the Assessment itself. This guidelines for the conduct of a DPIA are hence very short and concise.

Practical examples as to the application and benefits of the DPIA

Why can conducting a DPIA bring real benefits to data controllers can be seen form these real life examples:



Who can conduct a DPIA?

There are **internal and external DPIAs.** The internal PIA is conducted by the controllers of personal data themselves, whereas with external DPIAs company hires an **external consultant** or consults with the competent authority for the protection of personal data.

These **guidelines are intended primarily for the internal conduct of PIAs,** the result of which can also become an input in any procedure started by Directorate for Personal Data Protection (hereinafter DZLP). The persons involved in conducting a PIA should include appropriate legal and technical staff of data controllers and data protection or compliance officer(s). PIA report should be submitted to the management.

VI. HOW TO CONDUCT A DPIA!!!

DPIA Models

There are various models and approaches to conducting DPIAs and no single model of PIA which could be applied in all situations. There are very extensive DPIAs well as foreshortened ones, there are also DPIAs which can be applied in certain specific environments. Accordingly, the following can be differentiated:

a) a full-scale PIA;
b) a small-scale PIA;
c) check lists for compliance with legislation regulating the field of privacy; and
d) check-lists for compliance with legislation regulating personal data protection.

The approach taken in this guideline is the one of **small-scale DPIAs in combination with compliance check-lists.** These represent the best ratio between procedural formality and efficiency during this period when formal DPIAs are just beginning to become established. Small-scale DPIAs represent a smaller administrative burden and are most appropriate in relation to individual projects.

Conduct of the DPIA

A DPIA should have the following phases:

- preliminary phase risk identification,
- implementation of measures,
- final report

These can be integrated in into **a condensed check-list.** By means of a check-list, an organization should be able to:

- timely **identify the relevant legal obligations and risks** deriving from unlawful processing of personal data and non-compliance with ZVOP-1;
- **identify measures for avoiding or decreasing risk**, such as the use of anonymised data, minimization of the scope of data, minimization of retention periods, etc.;
- use it as a reminder in order not to neglect an important requirement of the law.

DPIA CHECKLIST

The purpose of the DPIA checklist is to draw attention, in a simple and transparent manner, to some of the most important elements of legislation as well as to some other critical issues, the address of which can potentially avoid subsequent troubles through the timely identification of risks. It should also be pointed out that this check-list only refers to LAW ON PERSONAL DATA PROTECTION and the fundamental principles of personal data protection; nevertheless, the **examination of all pertinent legislation is necessary** in relation to any consideration of the processing of personal data.

The check-list commences with the creation of a **project identity card,** by way of which it is decided what personal data shall be processed**,** by whom, when, and under what circumstances.

The most important elements of personal data protection, such as legal basis and personal data security, shall not be forgotten in the continuation.

Potential risks can be identified and avoided - or at least diminished - through the timely analysis of all the characteristics of the project in relation to the check list.

How formally should the check-list be applied? This decision is left to you; it is recommended that you use it to prepare the core of a written report or you can use it as a reminder in order not to neglect an important requirement of the law.

DATA PROTECTION AND PRIVACY IMPACT ASSESSMENT

DESCRIPTION OF THE PROJECT	Describe the project in a couple sentences (what are the main goals of the project and the main personal data processing operations).
RESPONSIBLE PERSON FOR THE DPIA	name and surname, position

CHARACTERIZATION OF INFORMATION	
We will collect, use, disclose or process the **following categories of personal data:**	name and surname telephone number e-mail address age gender items bought…
The **sources of information** are:	obtained from the individual directly obtained indirectly from other individuals publicly available data telephone registry other…..

LEGAL GROUND	
Legal ground is provided under.	Article 6, Line ☐ (e.g.consent of the personal data subject) Article 8, Line ☐ (…)
The following **specific legal conditions** define collection or further processing of information (authorities, legislation, agreement, etc.)?	write down the relevant sector-specific laws and concrete articles where possible
We need an **approval before processing** particular categories of personal data.	☐ yes ☐ no (exemption under Article 29, paragraph __)
We will obtain the following **approvals before processing particular categories of personal data (Article 29).**	☐ personal identification number of the personal data subject; ☐ data regarding the racial or ethnical origin of the personal data subject;

	☐ genetic data, except if the data processing is no performed by experts for the needs of the preventive medicine, medical diagnosis or nurture and therapy of the personal data subject and ☐ biometric data, necessary to confirm the identity of the personal data subject. ☐ data processed under Article 8 paragraph 2 line 1 (explicit consent) ☐ data processed under Article 9 paragraph 1 line 1 (explicit consent)

CONSENT	
Consent is obtained directly from an individual.	☐ yes ☐ no
Consent requires a **positive action by the individual**, rather than being assumed as the default.	yes: clicking the link in the e-mail / filling and signing a form/ clicking the check box/etc.

INFORMATION TO DATA SUBJECT	
Notice was provided to the individuals (data subjects) **prior to collection** of data?	☐ yes ☐ no
Individuals have the opportunity and/or right to **reject** to provide information.	☐ yes ☐ no
When the data are collected from the personal data subject, the latter is **informed on**:	(Article 10)
- the **identity** of the controller and of its authorized representative in the country, if any;	☐ yes ☐ no
- the **purposes** of the processing;	☐ yes ☐ no
- the **users** or categories of users of personal data;	☐ yes ☐ no
- the **compulsoriness** of responding to questions;	☐ yes ☐ no

- possible **consequences** of not responding and - **existence of the right** to access and the right to correct his/her personal data.	☐ yes ☐ no ☐ yes ☐ no
When the data are not collected from the data subject, disclosed we inform the personal data subject on: - the identity of the controller and of his/her authorized representative in the country, if any; - the purposes for the processing; - the data categories; - the users or categories of users of the personal data and - the existence of the right to access and the right to correct the data referring to the personal data subject.	 ☐ yes ☐ no ☐ yes ☐ no ☐ yes ☐ no ☐ yes ☐ no ☐ yes ☐ no
This information is provided at the time of recording the personal data or if disclosure of the personal data to a third party is envisaged, no later than the time when the data are firstly disclosed.	☐ yes ☐ no

USES OF INFORMATION	
Personal data will be used for the following **purposes**:	- Purpose A – sending commercial e-mails - Purpose B – on-line publishing - Purpose C – …. -
Data subject is aware of **all the purposes.**	☐ yes ☐ no

DATA MINIMIZATION AND PROPORTIONALITY	
We can achieve our goals **without** processing personal data.	☐ yes ☐ no
We can achieve our goals with:	☐ anonymous data ☐ aggregated data

	☐ statistical data
We can use **pseudonymous** data instead of raw data.	☐ yes ☐ no
We can use **one way hashing algorhytms** instead of raw data.	☐ yes ☐ no
The **minimum array** of personal data that is necessary in order to achieve our goals is:	compile a list of necessary personal data
It is necessary to use **unique identifiers** (e.g. National ID numbers or tax numbers).	☐ yes ☐ no
It is necessary to use **sensitive** personal data.	☐ yes ☐ no

ACCURACY OF INFORMATION	
The information will be **checked** for accuracy.	by insight into ID card, copying an ID card, etc…
The information will be **updated** by:	no ned for update/ checking with central registry…
The following steps shall be taken to ensure that the personal information is accurate, complete and up-to-date:	briefly describe the process

ACCESS TO DATA, CORRECTION OF DATA	
We have defined the **procedure** when the individual may access, assess and discuss or dispute the accuracy of the record.	☐ yes ☐ no
We have defined the **procedure for correcting inaccurate or erroneous data.**	☐ yes ☐ no
The **person in charge** for data subject requests is defined.	responsible person for database X / data protection officer …
Timeframes to deliver information are in line with provisions of the law.	see Chapter IV
The system designed to ensure that access by an individual to all of their personal information is simple.	☐ yes ☐ no

DATA RETENTION	
Personal data are retained:	
Category 1	x days/months/years/until consent is requested by data subject/ until contract is valid
Category 2	x days/months/years/until consent is requested by data subject/ until contract is valid
Category n	x days/months/years/until consent is requested by data subject/ until contract is valid

PERSONAL IDENTIFICATION NUMBERS	
We will process **personal identification number** of the citizen	☐ yes ☐ no
…and have one of the following **legal ground**	☐ yes ☐ no
prior explicit consent of the personal data subject;	☐ yes ☐ no
processing is necessary for the purpose of fulfilling rights and obligations of the personal data subject or controller, determined by **law**	☐ yes ☐ no
other case determined by law (which law).	☐ yes ☐ no (name of the law_____)

VIDEO SURVEILLANCE *(if applicable)*	
We have checked and apply the conditions set in **RULEBOOK ON THE CONTENT AND FORM OF THE ACT FOR THE MANNER OF PERFOMING VIDEO SURVEILLANCE.**	☐ yes ☐ no
We have prepared the necessary **notifications.**	☐ yes ☐ no
The **notifications** are: comprehensive	☐ yes ☐ no

visible positioned at the point the individual comes under surveillance	☐ yes ☐ no ☐ yes ☐ no
The notification contains the **required information**: the fact that video surveillance is being performed, the name of the controller performing the video surveillance and regarding the place and period of preserving the videos.	 ☐ yes ☐ no ☐ yes ☐ no ☐ yes ☐ no
The **aim of the video surveillance** is	☐ protection of the human life and health; ☐ property protection; ☐ protection of the life and health of the employees due to the job nature ☐ provision of control over the entry and exit from the official or business premises.
We have **other aim** of the video surveillance **not stipulated by the law.**	☐ control over employees ☐ ascertaining diligence at work ☐ other_____
Retention period of images does not exceed **30 days.**	☐ yes ☐ no
We have legal ground for **longer retention period** of images.	☐ yes ☐ no (name of the law_____)
We have adopted **a special act** regulating the manner of performing video surveillance.	☐ yes ☐ no (name of the act_____)
We have **notified the employees** for the performance of video surveillance in the official or business premises.	☐ yes ☐ no
We have checked that there is **no video surveillance** in dressing rooms, fitting rooms, toilets and bathrooms, elevators and other similar areas.	☐ yes ☐ no

DATA SECURITY	
We have checked and apply the conditions set in **RULEBOOK ON TECHNICAL AND ORGANIZATIONAL MEASURES FOR PROVIDING SECRECY AND PROTECTION OF PERSONAL DATA PROCESSING.**	☐ yes ☐ no
If transferred via electronic telecommunications network **special categories** of personal data will be protected by proper methods, therefore not being readable in the transfer process.	☐ yes ☐ no describe the method, e.g. HTTPS will be used to access to health data
Only the person with authorization from the controller or processor, including the processor himself, will process personal data. **Authorized persons** - have been **introduced with the principles** for personal data protection prior to accessing the personal data; - have been informed to perform personal data processing **in accordance with the directions** received from the controlled, unless otherwise regulated - have been informed to **preserve the personal data as confidential**, as well as the measures for their protection.	☐ yes ☐ no ☐ yes ☐ no ☐ yes ☐ no ☐ yes ☐ no
We keep **records for persons authorized** for providing personal data processing, containing: - name and surname of the authorized person; - date of issuance, expiry date, as well as scope of authorizations for approach to the personal data - access manner.	 ☐ yes ☐ no ☐ yes ☐ no ☐ yes ☐ no
Our **contractual processor** keep records for persons authorized for providing personal data processing, containing: - name and surname of the authorized person; - date of issuance, expiry date, as well as scope of authorizations for approach to the personal data - access manner.	 ☐ yes ☐ no ☐ yes ☐ no ☐ yes ☐ no

DATA PROTECTION OFFICER	
We have appointed a personal **data protection officer**.	☐ yes ☐ no
The **duties** of the personal data protection officer are in line with the requirements of the law.	see Article 26-1

OUTSOURCING /PROCESSING BY PROCESSORS	
We have signed a **written agreement** with all data processors.	☐ yes ☐ no
The **rights and obligations** are a part of the agreement.	☐ yes ☐ no
The Agreement contains the obligation of the processor to **act solely in accordance with directions** received from the controller.	☐ yes ☐ no
The Agreement contains the obligation for the processor to undertake **technical and organizational measures** to provide secrecy and protection of the personal data processing.	☐ yes ☐ no
We have determined the **manner of testing of the procedures** of the processor during the processing of the personal data.	☐ yes ☐ no

NOTIFICATION TO THE DZLP	
We will **notify** the Directorate before processing personal data.	☐ yes ☐ no
The notification contains the **prescribed elements as per Article 27(2).**	☐ yes ☐ no
An **exemption for notification is provided (Article 28)**	
- personal data are part of the publicly available collections based on a law;	☐ yes ☐ no
- personal data collection refers to at most ten employees with the controller	☐ yes ☐ no
- the processing refers to personal data of member of associations founded for political, philosophical, religious or trade union purposes.	☐ yes ☐ no

TRANSFER TO THIRD COUNTRIES	
We have checked and apply the conditions set in **RULEBOOK ON THE FORM AND CONTENT OF THE FORM FOR RECORD OF PERFORMED PERSONAL DATA TRANSFER TO THIRD COUNTRIES AND FOR THE MANNER OF KEEPING RECORDS**.	☐ yes ☐ no
We have a definite list of third countries where personal data will be exported to.	☐ yes ☐ no (name the countries)
Personal data will be transferred to third countries under provisions of Article 33.	☐ yes (Paragraph__) ☐ no

REVEALING PERSONAL DATA TO USERS	
Personal data will only be revealed on **user's written** (or electronic means in accordance with law) **request**, if needed for performing matters within legally determined competencies of the user.	☐ yes ☐ no
The **responsible person for handling user request** is defined	☐ yes ☐ no
The responsible person will **check**: - validity of the reason for request - legal basis for usage of personal data - personal data category being requested	 ☐ yes ☐ no ☐ yes ☐ no ☐ yes ☐ no
We have **determined a procedure to anonymize** personal data for **scientific**, **research** and **statistical purposes.**	☐ yes ☐ no Describe the procedure.
We keep separate records on the personal data which are revealed for usage, for the user of personal data and the reason for the revealing these personal data to the user.	☐ yes ☐ no

REFERENCES

1. Cavoukian, A., Taylor, S., Abrams, M.E.: Privacy by Design: essential for organizational accountability and strong business practices. Springerlink.com, June 2010.

2. Cavoukian, A.: Privacy by Design .... take the challenge. Information and Privacy Commissioner of Ontario, Canada. February 2009.

3. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union. COM(2010) 609 final. Brussels 4.11.2010.

4. ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications [of March 31, 2010]. ENISA, July 2010. http://www.enisa.europa.eu/

5. Gilbert, F.: The European Commission's proposed changes to the EU data protection regime and their consequences for businesses. World Data Protection Report, Vol. 10, No.12, December 2010.

6. Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications. The Article 29 Working Party, WP 180, Brussels, 11 February 2011.

7. Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance. WP 29, document no. 11750/02/EN, WP 89, Brussels, February 2004.

8. Paul,J.: The European Commission Enters Into a Privacy and Data Protection Impact Assessment Framework for RFID Applications: A Smarter approach to regulating Smart tags. World Data Protection Report, Vol.11, No. 4, pp.9-11, April 2011.

9. Privacy and Data Protection Impact Assessment Framework for RFID Applications. European Commission, 12 January 2011.

10. The Privacy Impact Assessment (PIA) Handbook. The Information Commissioner's Office. U.K. June 2009. 2nd edition. (http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx)

11. Privacy Impact Assessments. A guide for the Victorian public sector. Office of the Victorian Privacy Commissioner. Edition 2, April 2009.

12. Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act.

Ontario Information and Privacy Commissioner, Ontario, Canada, 2005.

13. Privacy Impact Assessment Handbook. Office for the Privacy Commissioner, Auckland, New Zealand, June 2007.

14. Privacy Impact Assessment. Mass Communication System. Office of Thrift Supervision. USA, 2009.