
"Let's collect this data too - we might need it one day."
"The online system wouldn't let me continue without this info."
"Legal basis? What legal basis? This isn't personal data, is it?"
"Well, that's what this form requires – you have to fill-in all the data."

Objective:	The purpose of these guidelines is to present Privacy Impact Assessment as an identification, analysis and risk-reduction tool for the purpose of lawful processing of personal data within the scope of e-Government development strategy implementation.
Target audience:	Policy-makers, personal data controllers, service developers, providers of information and communication technologies as well as other stakeholders in e-Government development strategies.
Sector:	Public
Version:	1.0
Published:	22.7.2010
Authors:	Information Commissioner RS
Key words:	Guidelines, Privacy Impact Assessment, PIA, privacy by design, personal data, connecting, e-Government, Strategy on IT and electronic services development and connection of official records (SREP).

CONTENTS

THE INFORMATION COMMISSIONER'S GUIDELINES **4**
INTRODUCTION **5**
CHAPTER ONE **6**
WHAT IS A PRIVACY IMPACT ASSESSMENT? **6**
Why are PIAs useful? 6
Practical examples as to the application and benefits of the PIA 7
Who can conduct a PIA? 8
What are the fundamental principles of the PIA? 8
CHAPTER TWO **12**
HOW TO CONDUCT A PRIVACY IMPACT ASSESSMENT (PIA) **12**
PIA Models 12
Conduct of the PIA 12
Check-list 13
CONCLUSIONS **26**
SOURCES & USEFUL LINKS **28**

THE INFORMATION COMMISSIONER'S GUIDELINES

The purpose of the Information Commissioner's guidelines is to provide common practical instructions for individuals whose personal data (PD) is processed, as well as for legal and other entities who process personal data compliant with the provisions of the Personal Data Protection Act RS (Official Gazette of the Republic of Slovenia, No. 95/07 – official consolidated text; hereinafter ZVOP-1).

The legal basis for the Information Commissioner's issue of these guidelines is provided by Article 49 of the ZVOP-1 which stipulates that the Information Commissioner RS shall provide non-binding opinions, explanations and positions regarding personal data protection, and, further to this, publish these on its website or in other suitable formats, as well as prepare and offer instructions and recommendations regarding personal data protection in individual areas.

See also:

- Information Commissioner's opinions: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/
- Information Commissioner's brochures: http://www.ip-rs.si/publikacije/prirocniki/

The Information Commissioner's guidelines are published on its website:
http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

INTRODUCTION

SREP – Slovenia's **Strategy on IT and Electronic Services Development and Connection of Official Records** - was adopted in June 2009 for the purpose of setting the framework and goals for further implementation of new and already existing development activities in the field of electronic services in public administration. In the chapter on provision of horizontal functions, SREP foresees the preparation of common methodologies and policies (Chapter 6.5.4.), among which preparation of **methodology for undertaking a privacy impact assessment** has also been foreseen.

Improving the performance and efficiency of the public sector and the development of e-Government services requires the ever more wide-ranging and intensive connection of state-public sector data sources which encompass extensive personal data filing system filing systems. In this, the state immediately faces a dilemma as to how to fulfil its mission whilst respecting fundamental human rights, including protection of privacy of the individual against excessive and illegal interventions by public administration and the state. Within the context of numerous informatization projects, the connection of data sources, the development of new services and – last, but by no means least - proposals for amendments of legislation, care for protection of privacy and personal data is neglected; and only later during inspection procedures, irregularities or illegalities are being discovered. The price of eliminating misdeeds and taking over responsibility may be high, as well as involve a loss of time and a loss of reputation. Privacy impact assessments are a tool which may help us avoid such situations.

Privacy Impact Assessments - PIAs - have proven to be an efficient tool through which one can, in a timely manner, **identify risks and requirements** stipulated by legislation in relation to the processing of personal data. Breaches of legislation, losses of reputation together with the inefficient and inexpedient use of resources can also be avoided through the implementation of PIAs. Privacy Impact Assessments can be time consuming and demanding from an administrative perspective, however, in the Information Commissioner's opinion the efficiency of such a tool shall be balanced and optimized through the necessary input and administrative burden. The Information Commissioner's guidelines are hence short, concise and focused on efficiency and minimization of the means necessary for their conduct.

CHAPTER ONE

WHAT IS A PRIVACY IMPACT ASSESSMENT?

A Privacy Impact Assessment - PIA[1] is an identification, analysis and risk-reduction tool which may be used to avoid illegal personal data processing, which can occur during implementation of any project, system or technology. Such assessments are more established in those environments where the legislative and the supervisory emphases lie on the protection of privacy and not so much on the safeguard of data protection. Privacy impact assessments are also a frequently used (and sometimes mandatory) tool for policy-makers, creators of legislation and projects in countries as Canada, Australia and the USA, and now they are slowly making their way into the European arena, where we put a larger emphasis on the protection of personal data[2]. They are used in the public as well as in the private sector; moreover, wherever they have been introduced, they have become established and remained in use.

PIAs are based on the systematic and timely identification of risks emanating from unlawful processing of personal data; they can be used for the early detection of risks and their easier elimination, reduction or acceptance thereof. In a way, PIAs are similar to Information Commissioner's inspection procedures where it is assessed to what extent personal data processing is compliant with ZVOP-1, whereas the purpose of the PIA is prior risk analysis, as well as optimization of procedures for achieving compliance.

Why are PIAs useful?

The Information Commissioner has, in its 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 PIA before implementing a certain project or before using a certain technology. In such a way the PIA 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:

[1] For more on the historical background and characteristics of the PIA see: http://www.rogerclarke.com/DV/PIAHist-08.html.
[2] Particularly following the adoption of Directive 95/46 ES on personal data protection.

- 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 fulfil a project's objectives in a manner which does not require e 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 ZVOP-1.

By conducting the PIA, 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 PIA 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. The guidelines for the conduct of a PIA are hence very short and concise.

Practical examples as to the application and benefits of the PIA

Cited below are three real life examples encountered by the Information Commissioner

- Connection of personal data fining systems from official sources and public records in the public sector, without previously obtaining a mandatory approval from the Information Commissioner; any such action, without obtaining prior consent from the IC, represents an offence by the data controllers.

- A public transport e-ticketing system recorded data on the time and location where passengers entered a bus, which in itself represented disproportionate processing of personal data – as a consequence expensive and time-consuming corrections needed to be made to the IT system.
- A retailer who issues loyalty cards, planned to collect personal data on customers purchase habits – upon conducting a PIA, the retailer timely stopped with the execution of his plan, which included sole notification to the customers as to the intended collection of personal data with an expectation of an implied consent. Instead the merchant correctly introduced a system for the collection of *explicit consent* (*opt in* as opposed to *opt out)* from individual customers; this way the retailer saved itself from a potentially high fine as well as from requests for data erasure.

Who can conduct a PIA?

There are **internal and external PIAs;** both are already being conducted in Slovenia at a more informal level. The internal PIA is conducted by the controllers of personal data themselves, whereas with external PIAs a company hires an external consultant or consults with the competent authority for the protection of personal data – the Information Commissioner. The Information Commissioner issues non-binding written opinions and there is also the possibility to consult IC experts prior to the introduction of any project which involves elevated risk in relation to the protection of personal data. The Information Commissioner publishes and makes available to the public sector bodies and authorities its guidelines and decisions as to the compliance of a proposed statute with laws and other regulations regarding personal data protection. This modus operandi is increasingly being augmented and observed.

All of these **guidelines are intended primarily for the internal conduct of PIAs,** the result of which can also become the subject of a later consultation with the Information Commissioner.

What are the fundamental principles of the PIA?

The basic principles of the PIA build on the fundamental doctrine of the protection of personal data.

Lawfulness

The principle of lawfulness means that the general rules for personal data processing (and especially such issues as the scope of personal data and the objectives of processing) shall be prescribed by law. The lawfulness of personal data processing means that personal data in Slovenia (pursuant to the second paragraph of Article 38 of the Constitution of the Republic of Slovenia) can only be processed in compliance with law, and/or on the basis of a general authorization arising from law. The latter is particularly germane for legal entities under private law, for which a general authorization and the general rules are for the most part predetermined by statute, namely ZVOP-1, while more detailed rules may be stipulated by way of personal consent of the individual concerned, or a contract, or a similar agreement. As a rule, processing of personal data in the public sector must be defined by law.

Honesty and transparency

Honesty and transparency logically refer to the fact that processing of personal data must be conducted in a manner which is honest and apparent to the individual. In addition to knowing by whom and under what conditions their data will be proceeded, each individual must be aware as to what personal data will be processed, who will process it, and for what purposes. In the public sector, these principles shall be ensured by respecting the rule of law; in the private sector the appropriate informing of an individual is essential, so that they might - on the basis of sufficient information - provide their consent, or withhold their consent, for certain personal data to be processed for certain predetermined purposes.

Proportionality

Proportionality means that it is only permissible to collect and to process the **smallest scope of personal data necessary to achieve the purpose of processing** personal data. Proportionality may primarily mean that if such **personal data is not necessary to achieve the goal, then it is not appropriate to collect it.** Besides to the scope of data, proportionality also refers to the use of less sensitive data. In case of abuse the consequences thus may not be as great (pseudonyms are better than explicit identifiers, whilst random strings of code are better than unambiguous indicators). Proportionality also refers to the temporal aspect: any excessively long retention or processing of personal data is inadmissible; data should be erased, destroyed or anonymised after the purpose of processing has been achieved, or after the legally or otherwise defined deadline has expired.

Some very obvious examples of disproportionality include:

- Requiring a personal identification number (EMŠO) when buying bread;
- Storage of data on time and location when a monthly- or travel-card carrying passenger enters a city bus;
- Requiring multiple unique identifiers (e.g. personal identification number and tax number at the same time) ;
- Storage of data without a valid purpose, and merely for reasons of stock;
- The collection of unnecessary data (”*The on-line system would not let me continue without providing all this information” “This is our standard form”, “Just complete this in full*…”)

Accuracy and contemporaneity

The principles of accuracy and keeping up-to-date dictates that the data being processed must be correct and current. Accuracy means that the data is not erroneous or incomplete, whereas keeping up-to-date means that the most recent data is used. Personal data may be accurate but not up-to-date, which means that data is used which is accurate and valid at a certain point in time; however, newer and more up-to-date data is also available. The frequently iterated argument ‘*I have got nothing to hide*’ is quickly diluted if the principle of accuracy and keeping up-to-date is not respected, and your data in certain records becomes erroneous or inaccurate.

Retention period

Retention is likewise connected to the principle of proportionality. Personal data may only be stored for the period of time required to achieve the purpose for which the data has been collected and further processed. After having fulfilled the purpose of processing, personal data should be deleted, destroyed, blocked or anonymized, unless such data has been categorized as archival material under the provisions of the law regulating archival materials and archives, or it is retained under the tenets of other legislation which mandates the retention of certain personal data.

One of the essential elements of the PIA is the examination and designation of an appropriate retention period, whereby such a retention period may already be laid down by law; it is, however, essential, that the retention period is not open, but unambiguously defined.

Personal data security

Personal data security is a narrower term than the protection of personal data, and refers to organizational and technical measures by means of which personal data is made secure; thus personal data security represents the prevention of accidental or intentional unauthorized destruction of data, its amendment or loss, as well as the unauthorized processing of data. In other words: our personal data can be exceptionally well protected under a competent data security system; this said, however, personal data is still open to abuse, particularly so if other principles are not taken into consideration (e.g. data processing without a legal basis, its application for purposes other than that which it was specifically collected, as well as the excessively long retention of data and suchlike).

Observing the rights of the individual

One of the essential principles of personal data protection refers to the rights of individual whose personal data is processed by a data controller in the public or private sector. Any individual namely enjoys the right to examination of his/her personal data and, in the event of established irregularities, also enjoys the right to object as well as require correction, blockage or deletion of erroneous data.

CHAPTER TWO

HOW TO CONDUCT A PRIVACY IMPACT ASSESSMENT (PIA)

PIA Models

The Information Commissioner has examined various models and approaches to conducting PIAs, further to which it establishes that there is no single model of PIA which could be applied in all situations. There are very extensive PIAs as well as foreshortened ones, there are also PIAs which can be applied 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 Information Commissioner hence proposes that those involved in e-Government projects use the approach described below, whereas the application of appropriately adjusted PIA guidelines is recommended in a variety of circumstances. **The Information Commissioner** prepared guidelines based on **practical experience in relation to informal Privacy Impact Assessments already conducted**, for **small-scale PIAs in combination with compliance check-lists.** The IC is of the opinion that these represent the best ratio between procedural formality and efficiency during this period when formal PIAs are just beginning to become established. Small-scale PIAs represent a smaller administrative burden and are most appropriate in relation to individual projects.

Conduct of the PIA

The Information Commissioner recommends consolidation of the usual phases of the PIA (preliminary phase risk identification, implementation of measures, final report) 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.;
- obtain referral to more detailed information in already published materials (legislation, guidelines, and alike).

PIAs and ISO 27001 - the information protection standard

Risk analyses in PIAs basically have a broader scope than those required by the essential phase in accordance with the ISO 27001 information protection standard. PIAs are based on fundamental principles of personal data protection, whereby data security, which is commensurate with the aims of information protection as per ISO 27001, is only one of the fundamental building blocks of personal data protection. The PIA namely examines whether excessive amounts of data are being processed, for what purpose the data is being processed, whether there exists a legal basis for the processing of personal data, as well as whether the data is appropriately secure. The segment of data security is the point of contact between the PIA and the ISO 27001 standard, and it is here that the subdivisions of ISO 27001 - such as risk analysis and the risk treatment plan - excellently coincide with the legal requirement of a suitable degree of personal data security.

Check-list

The purpose of a check-list 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 ZVOP-1 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.

All 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 shall the check-list be applied?

This decision is left to you; answers can be found to all these elements in relation to any project, and these should be written down. The checklist may alternatively be used merely as a reminder. Whilst it is essential not to over exaggerate the formality, it is also crucial that none of the important aspects are overlooked.

		Detailed explanation	More information
PROJECT IDENTITY CARD	Scope of personal data	The scope of personal data which is going to be processed shall be determined as early as possible. Special attention must be paid to the following: • **processing** - which means **any handling of personal data;** • personal data is any data which refers to an **identified** or **identifiable person**; • identifiability should not merely be considered in relation to our own capacities, capabilities, information and knowledge - but also to those of others. Could any other person determine to whom the data refers, without resort to disproportionate effort, time or means? • ZVOP-1 covers any personal data which is **part of a filing system,** or which is **intended for inclusion in it;** • there must be a **legal basis** for the processing of personal data.	If you need an answer to a particular question, check, if somebody has already asked that same question: See: Opinions of the Information Commissioner: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/ Guidelines of the Information Commissioner: http://www.ip-rs.si/varstvo-osebnih-
	Handling personal data	Think it through and write it down: • how will the personal data be obtained (from official records / from individuals / in electronic form / on paper/ …); • where is the data going to be stored (in an information system / in folders / …); • to whom will this data be transferred (to other authorities / users / …),	

		• who is going to work with the personal data (which departments and people); • how is the data going to be protected against accidental or intentional misuse, loss or destruction (technical / organizational issues); • for how long is the data going to be stored; • how is the data going to be destroyed after the expiry of processing period (under commission / in house/ by a contracting partner)…	podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/
	Legislation	Check the provisions of the pertinent legislation governing processing of personal data, in particular from the perspective of the following: • purpose of processing, • scope and range of data, • retention period, • security requirements, • data availability conditions and alike.	
	Proportionality	The legislator has considered the principle of proportionality in its creation of the legal bases. In any project, the responsible persons must determine the **minimal sufficient scope of personal data which is required to achieve the purpose of processing:** • if certain personal data is superfluous or unnecessary, then it shall not be collected (**anonymized** or **statistical data** is often sufficient); • if personal data is necessary, then the least sensitive data should be utilized; multiple unique identifiers must not be collected unless absolutely necessary.	See: Article 3 of the ZVOP-1

	The range and scope of personal data shall be kept to a minimum. Proportionality – and the notion of Privacy by Design – shall be observed in all phases: • In the design of search engines (designation of the possible search criteria; determination as to the scope of search results displayed). • Determination of users' rights (access level - whether a given user really needs access to certain data); the greater the data provided, the higher the requirements as regards traceability! **ACCESS TO PERSONA DATA** **WRONG: Everybody, everything, always, and without trace!** **RIGHT: Designated persons, minimal data, and traceability!** Wherever possible – maintain the personal data of an individual, under the control of that individual! (it is both fair and proportional to have biometric samples, data on location etc. on a card, with which the individual themselves disposes). The risk of abuse can be reduced through avoiding the centralized storage of data.	
Legal basis	A legal basis for the processing of personal data may be provided by statute or the personal consent of the individual concerned. The legal basis for public sector operators is defined in more detail in Article 9 of the ZVOP-1. ATTENTION!	See: Article 9 of the ZVOP-1 legal bases in the public sector

	A **special legal basis** or a **Decision issued by the Information Commissioner** is necessary for certain types of processing – such as those involving the application of biometrics, the connecting of filing systems, and the export of data to third countries. If the legal basis is the **consent of an individual,** then it is important to: • examine the manner of obtainment, evidence-taking and the means of revocation of consent; • consider that a lack of response shall not be regarded as a silent consent of an individual; • consider that personal consent shall only be regarded as the voluntary and free statement of an individual that their personal data may be processed for specific purpose; • consider that an individual being **well-informed is merely a precondition** for the legal basis, and is not a substitute for the free and voluntary consent of that individual; • consider that the personal consent of an individual may be written, oral or some other appropriate authorization provided by that individual (e.g. a click on a link or a button on a website); • be aware that the correct way to set-up confirmation windows on websites shall be that those windows are, by default, empty and not pre-ticked.	
	If certain operations involving personal data are conducted by a contractual processor, then the requirements of Article 11 of the ZVOP-1 must necessarily be observed: **the contract must be concluded in writing** and encompass **predetermined procedures**	See: Article 11 of the ZVOP-1

Contractual processing	**to be undertaken by the contractual partner for the protection of personal data.** ATTENTION! Processing personal data – shall be defined as any operation or set of operations performed in connection with personal data. Even filing, sending or the destruction of data shall be regarded as processing personal data, and whether or not a contractual processor knows to whom the data pertains is unimportant in consideration as to whether processing has taken place! Contractual processing should also be observed through the eyes of the individual: **Is there a possibility of abuse of personal data by the contractual processor**? You have both the right and duty to **supervise** a contractual processor, since they are the proxy in the processing of sensitive data! The contractual processor should safeguard personal data in the same manner as would the data controller. ATTENTION! The employees of a contractual processor must receive detailed instructions on what they may and may not do with personal data!	
Accuracy and keeping personal data up-to-date	Personal data needs to be accurate and kept up-to-date. A data controller may, prior to input into a filing system, verify the accuracy of personal data by examining an identity document.	See: Article 18 of the ZVOP-1

Informing the individual	An individual needs to be appropriately informed as to the processing of their personal data. If personal data is collected directly from the individual to whom it relates, the data controller or its representative must specifically ensure communication of the following information to the individual: • **information about the data controller** and its representative (persons name, or official title, and address) • **the purpose of** personal data **processing.** On occasions, other information may also need to be provided if legal and fair processing is to be ensured. (See: Article 19 of the ZVOP-1). An appropriate privacy policy or other **declaration on the protection of personal data** needs to be designed for websites.	See: Article 19 of the ZVOP-1 See: Smernice Informacijskega pooblaščenca za oblikovanje izjave o varstvu osebnih podatkov na spletnih straneh
Use of the same connecting codes	The same connecting codes are for example: **unique personal identification number (EMŠO), tax number, national health and social security number.** In the acquisition of personal data from filing systems in spheres as health, social security, the police, national intelligence - security, defence, the judiciary and criminal justice and records, the same connecting code may not be used for the purposes of obtaining personal data. Exceptions are possible.	See Article 20 of the ZVOP-1 See Guidelines: Varstvo osebnih podatkov pri povezovanju zbirk osebnih podatkov v javni upravi

	Search engines and the use of various coding tables need to be appropriately adjusted!	
Retention period	Personal data may only be stored for **as long as it is necessary to achieve the purpose** for which the data was collected or further processed. On completion of the purpose of processing, personal data shall be erased, destroyed, blocked or anonymised, unless - pursuant to the statute governing archive materials and archives – such is specifically defined as archive material, or unless the law provides otherwise for an individual type of personal data. If the law does not stipulate the retention period, then it is recommended to define it by observing the principle of proportionality – the shortest period that is necessary to achieve the purpose of processing. Erasure of electronic data needs to be appropriate (physical destruction under a designated commission; data carriers should be randomly overwritten several times etc.)!	See: Article 21 of the ZVOP-1
Supply of personal data	Personal data may be supplied to the users of personal data who enjoy the necessary legal basis for such.	See: Article 22 of the ZVOP-1
Security		

Internal regulations	Internal regulations shall define the procedures and measures for the security of personal data. When a new project is introduced, the internal regulations will need to be up-dated. Lawyers and IT experts should co-operate in the drafting of such internal regulations.	See: second paragraph of Article 25 of the ZVOP-1
Designation of responsible persons	The persons responsible for individual filing systems and the persons who have authorization to access personal data (access rights / security scheme) shall be defined, documented and updated.	See: second paragraph of Article 25 of the ZVOP-1
Internal traceability of processing	The system must enable the subsequent determination of when individual items of personal data were entered into the filing system, when they were used or otherwise processed, and who did so. Security needs to be - and must be allowed to be - adjusted to the nature and the risk that the processing of certain types of personal data engenders. In cases of sensitive personal data - i.e. with large filing systems of data as well as in instances where the risk of abuse or the 'value' of personal data is considerable - every individual insight into personal data should be traceable. Special attention should be dedicated to the supervision of system administrators as well as the authenticity of revision traces and daily activity logs.	See: Item 5, first paragraph of Article 24 of the ZVOP-1

	Risk analysis needs to be carried out, and security measures adjusted, for those collections which are maintained on paper (e.g. personnel records).	
Traceability of supply (external traceability)	For each instance of the supply of personal data it should be ensured that it is subsequently possible to determine what personal data was supplied, to whom, when and on what basis.	See: third paragraph of Article 22 of the ZVOP-1
Information Security Management System (ISMS)	The introduction of a **more comprehensive and systematic approach to data security** – such as the introduction of the Information Security Management System (ISMS) - should be considered for more complex projects. Recommendations on this are provided by ISO 27001.	See: http://en.wikipedia.org/wiki/ISO/IEC_27001
Appointment of a Data Protection Officer	The appointment of a Data Protection Officer – a responsible individual specialized in ensuring compliance with legislation – should also be considered when undertaking more complex projects.	
Internal supervision	Will any misuse or abuse of personal data be detectable? Will it be possible to differentiate whether employees access personal data for legitimate and legal purposes, or merely out of curiosity, or as a favour to a friend.	
Education	Personal data security is also predicated on the appropriate education and awareness of employees – the human factor is a frequent cause of misuse.	

	When employees and the employees of the contractual processors were last made familiar with the requirements of the ZVOP-1? - Are the internal rules just gathering dust?	
Information Commissioner's catalogues and register	A **catalogue** (description) of the design and content of the personal data filing system must be created in a timely fashion for each personal data filing system. Certain data need to be supplied to the **Information Commissioner for the purpose of the upkeep of the IC's register.** (See: http://www.ip-rs.si/varstvo-osebnih-podatkov/register-zbirk/). Timeframes, scope of data and exceptions are stipulated by statute.	See: Article 26 of the ZVOP-1 See: Article 27 of the ZVOP-1 For exceptions see: Article 7 of the ZVOP-1
Transfer of personal data to a third country	If personal data are going to be transferred to a third country which does not yet ensure an adequate level of personal data protection, then the transfer must be approved by the Information Commissioner. List of countries deemed to have an adequate level of data protection: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm	See: Articles 63 to 71 of the ZVOP-1

Video surveillance	ZVOP-1 stipulates the conditions regarding admissibility of the introduction of video surveillance. The issue of **proportionality** is crucial in relation to the introduction of video surveillance. Recording might not be necessary all the time, while recording shall be limited to those areas where such is necessary in order to protect property or people. Recording in working areas (offices, shop floor etc.) should be avoided unless there exist urgent or overriding reasons for such.	See: Articles 74 -77 of the ZVOP-1
Biometrics	ZVOP-1 stipulates special criteria as regards the admissibility of biometric measures. A prior positive decision is required from the IC prior to any introduction of biometrics, and such may only be used in relation to employees if they have been informed in writing thereof in advance; this is not in itself, however, a sufficient condition for the introduction of biometric measures.	See: Articles 78 – 81 of the ZVOP-1 See also: Smernice glede uvedbe biometrijskih ukrepov
Connection and integration of personal data filing systems	A special, explicit legal basis is required for the (inter-) connection or integration of personal data filing systems. Connection is not the same as the mere transfer of personal data A more detailed explanation of this issue is provided in the Guidelines.	See: Articles 84 – 86 of the ZVOP-1 See also: Smernice Varstvo osebnih podatkov pri povezovanju zbirk osebnih podatkov v javni upravi

CONCLUSIONS

As a tool for identification, analysis and diminution of risk in relation to unlawful personal data processing, Privacy Impact Assessments – PIAs – are still in their infancy in Slovenia. As such, these Guidelines represent one of the first such accessories in the Slovene milieu. This tool will undoubtedly be improved upon in the future, and it is the wish of the Information Commissioner that PIAs specifically adjusted to the needs of other fields and sectors (e.g. private sector) shall be developed in the future.

These Guidelines will have achieved their purpose if policy makers and those responsible for the creation of actual practical solutions within e-Government take them on board in good time, and in such a way avoid the unnecessary wasting of time, resources and reputation that shall derive from ill-conceived and erroneously implemented e-Government projects.

Through the respect of the concept of Privacy by Design, which is becoming one of the fundamental principles of the protection of personal data, these Guidelines also have a more idealistic and future-focused aim in the fight against the inconsiderate use of modern technologies, and with that the slide into a surveillance society.

SOURCES & USEFUL LINKS

- Office of the Privacy Commissioner of Canada – Privacy Impact Assessment Fact Sheet: http://www.priv.gc.ca/fs-fi/02_05_d_33_e.cfm

- Office of the Privacy Commissioner (UK) – Privacy Impact Assessment (PIA) Handbook (Version 2): http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

- Office of the Privacy Commissioner (UK) – Privacy by Design (Report): http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf

- Office of the Privacy Commissioner of Canada – Privacy Impact Assessments http://www.priv.gc.ca/pia-efvp/index_e.cfm

- Office of the Privacy Commissioner (New Zealand), Privacy Impact Assessment Handbook http://www.privacy.org.nz/library/privacy-impact-assessment-handbook

- Guidelines of the Information Commissioner (Slovenia): http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

- Opinions of the Information Commissioner (Slovenia): http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/