Guidelines for developing information solutions

Concerned about privacy?
Build it right in!

INFORMACIJSKI
POOBLAŠČENEC

The purpose of the document:	These guidelines address the most important requirements to be followed in the development of information solutions encompassing personal data processing. The guidelines are intended for all those involved in the development of solutions in the field of information and communications technologies or the commissioning of such, irrespective of whether new products, services, and systems, or individual solutions and applications are at issue.
Target public:	Developers of information systems, solutions, and applications and clients commissioning such services.
Status:	Public
Version:	1.0
Date of issue:	6 December 2010
Authors:	The Information Commissioner
Key words:	Guidelines, information system, application, personal data protection, traceability, proportionality, privacy by design.

TABLE OF CONTENTS

About the guidelines of the information commissioner

The purpose of the Guidelines of the Information Commissioner is to provide practical advice to individuals whose personal data are processed as well as to personal data controllers and processors. The Guidelines are intended to answer in a clear, understandable, and useful manner the most frequent questions related to individual topics regarding personal data protection. By means of such Guidelines the Information Commissioner wishes to foster better knowledge of and respect for information privacy and the provisions of the Personal Data Protection Act (Official Gazette RS, No. 94/07, official consolidated text, hereinafter: the PDPA-1).

The legal basis for issuing the Guidelines is provided for by Art. 49 of the PDPA-1, which, inter alia, determines that the Information Commissioner issues non-binding opinions, clarifications, and positions on issues in the area of personal data protection and publishes such on its website or in some other appropriate manner, and prepares and issues non-binding instructions and recommendations regarding the protection of personal data in individual fields.

See also:

- *Opinions of the Information Commissioner (in English):* https://www.ip-rs.si/index.php?id=383

- *Publications of the Information Commissioner (in English* https://www.ip-rs.si/index.php?id=388

The Guidelines of the Information Commissioner are published on the following website:

http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

Introduction

The introduction that follows is intended to be brief, clear, and understandable to readers. Contrary to the publicly voiced opinions of the CEOs of some of the largest Internet-based corporations, such as Facebook and Google, in our opinion the protection of privacy will remain an important societal norm. Nevertheless, it is no doubt true that information privacy is under constant threat in the era of the information society. Legislation cannot follow the rapid technological progress fast enough, and individuals' consciousness reacts to such with delay as well, such that they often use new tools without careful prior consideration. However, even careful consideration is often not sufficient, as the relevant privacy policies are often very long, the systems function on the basis of the principle that could be described as "everyone always has access to all data without control", applications retain data for possible future use, and large amounts of personal data are processed merely due to the transition from paper-based to electronic transactions, etc.

If privacy is to be preserved in the information society, certain principles must be respected. These Guidelines address such in a neutral manner from the perspective of the technologies used and address a wide range of related issues as they are intended for any one developing a product or service in the domain of the information society and related to personal data processing. Whether you are developing or introducing an electronic ticketing system for public transportation, a project enabling average speed measurement over a set distance on highways, a "pay-as-you-drive" vehicle insurance system, a new CRM system, a tool for managing mailing lists, a system for monitoring the purchasing habits of your clients, or similar, the present Guidelines apply to you. Prior consideration of legal conditions and respect for the Privacy by Design concept can save you money, raise your clients' trust in you, and protect you from violating legislation. The expected introduction of obligatory reporting on data security incidents in Europe (e.g. in the event you lose the data of your clients) and the costs arising from such will make the importance of the timely implementation of privacy into business practices ever more apparent. While privacy by design might also find a place in future European regulation of personal data protection, it is the cornerstone of the present Guidelines.

Privacy by design

The privacy by design concept is based on seven fundamental principles, as detailed below. Privacy embedded into design arose as a response to the requirements of Surveillance by Design – which developed in the mid-1990s when information and communication tools were supposed to be designed to enable prosecution authorities and intelligence agencies access to information . Implementation of the privacy by design concept should be recognised as a competitive advantage and a tool for raising individuals' trust; the concept will very likely be enacted also in future European legislation on personal data protection. In today's world, in which the law lags ever farther behind the rapid technological development (if we only remember how old Google and Facebook are and how different the world was 10 years ago), the privacy by design concept might be one of the tools that can help preserve our privacy in the information society.

The Privacy Impact Assessment (hereinafter: the PIA) and the use of Privacy Enhancing Technologies (hereinafter: PETs) are also closely related to the privacy by design concept. The PIA, which could be considered an element of the privacy by design concept, is a tool for the identification, analysis, and reduction of risks related to the unlawful treatment of personal data, which can occur with regard to individual projects, systems, or the use of technology. Such assessment is more established in those environments where legislative and supervisory emphasis is placed on the protection of privacy rather than on personal data protection. Thus, the PIA is a tool that is often used (and is sometimes even obligatory) by drafters of legislation, policies, and projects in Canada, Australia, and the USA; it is slowly making its way also into Europe, where there is greater emphasis on personal data protection . The PIA is used in the public as well as in the private sector, and wherever it has been introduced it has become established and permanent.

Therefore, the PIA is an essential element of the privacy by design concept, which is based on the following seven fundamental principles.

1. Proactive instead of reactive

The privacy by design concept is based on proactive behaviour, which entails avoiding problems instead of removing consequences. Instead of waiting for risks to materialise, potential problems regarding personal data and privacy protection should be envisaged early enough and the design of the system adapted in a manner that would decrease the risk of abuse. If the privacy by design concept is not taken into account in designing solutions, it will cost time and money, as well as one's reputation, to subsequently adapt to it; furthermore, in some cases making subsequent corrections to a system may cost more than terminating it and implementing a new one.

2. Privacy by default

Privacy-friendly settings should be set as the default in information solutions. The following are examples of such:

- tick-boxes and similar confirmation elements where individuals agree that their data may be processed should be empty by default – individuals should confirm their agreement actively, i.e. by filling in the field;
- default settings regarding whether data may be made publicly available (e.g. with regard to on-line social networks) should presume the confidentiality of data.

3. Privacy embedded into the design of a solution

Privacy should be embedded into the very concept and architecture of information solutions and business practices and not be added subsequently. Privacy must be considered already in the phase when the functionality-related requirements of the system are established and subsequent methods of ensuring privacy throughout the entire life cycle of the system must be envisaged.

4. Full functionality – not a zero-sum game

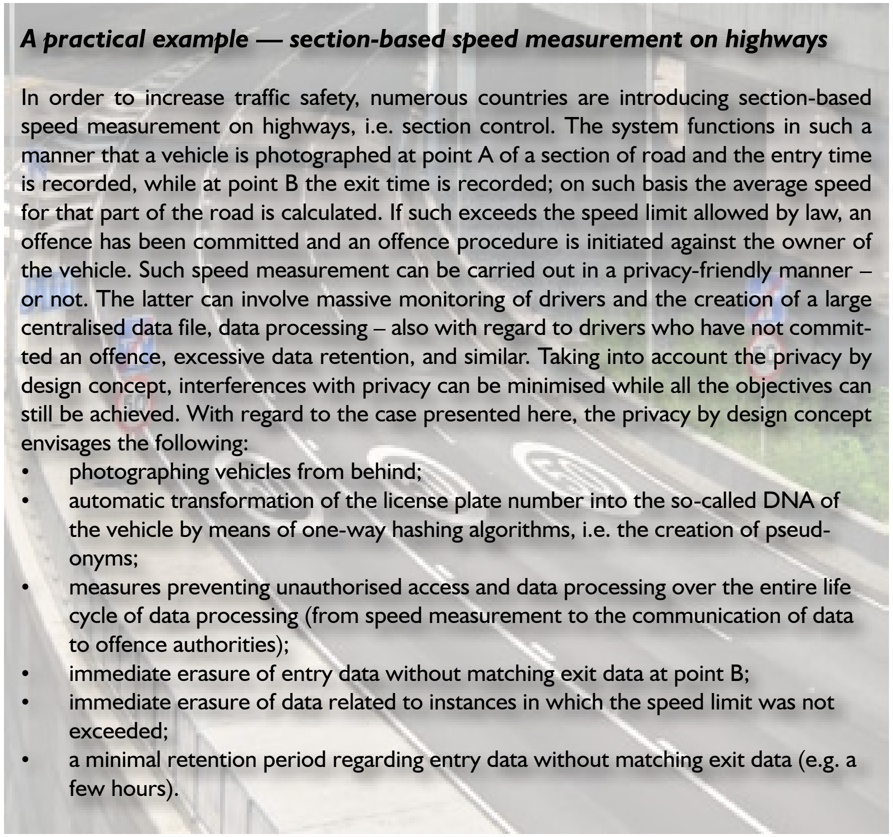
An essential element of the privacy by design concept is ensuring full functionality – the incorporation of privacy should not be at the expense of the effectiveness of the system or of other legitimate objectives. It can often be heard that one must give up privacy for the sake of a higher level of security, practicality, or economic efficiency, however, the basis of the Privacy by Design concept is finding solutions which do not force people to choose between the two options but which ensure both. And, yes, this, as a general rule, requires knowledge and time and resources; however, it is possible, also as a general rule, to do both – i.e. preserve privacy and still achieve the objectives pursued.

5. Ensuring data security over the entire life cycle of data processing

Data security is an important element of personal data protection and refers to the prevention of unauthorised personal data processing and accidental or deliberate personal data alteration or loss. Ensuring appropriate data security must be perceived as a process and not as individual tasks that are finished once they are completed. Personal data security processes must be founded on planning, implementation, reassessment, and appropriate reaction to detected irregularities and shortcomings. The Information Commissioner recommends that all data controllers follow the guidelines in international standards regarding the protection of information, such as those determined by the ISO/IEC 27000 family of standards, as well as that they periodically check for the presence of some known vulnerabilities , which can nullify the effect of other measures.

6. Transparency

Closed solutions which ensure personal data protection in a dubious manner and which are based on our trust in them, as it is not possible to check them, are not in accordance with the privacy by design concept. However, the opposite is true as well – solutions with privacy embedded into their design must enable independent external assessment and verification of the actual level of personal data protection they provide. Instances have occurred in the field of cryptography that entailed the application of hidden encryption methods which were, due to such confidentiality, allegedly safe; however, on numerous occasions it has turned out that only those solutions are truly safe that have undergone public assessment and that were "impossible to crack" even by the best researchers who had all the existing means available to them . An average developer is unlikely to be able to put together a secure cryptographic algorithm, which is why it is necessary to stick to proven encryption methods. Public assessment in itself is not a guarantee that a certain solution will be flawless from the perspective of security, however in certain cases public assessment should be necessary – such as the example of introducing smart personal identity cards in the future.



A practical example — section-based speed measurement on highways

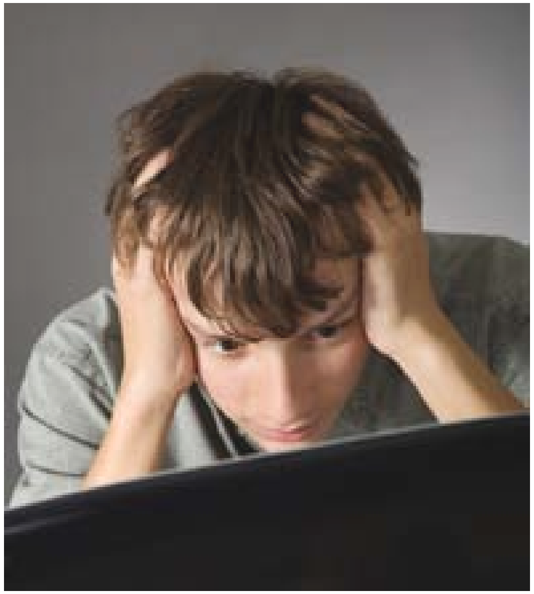
In order to increase traffic safety, numerous countries are introducing section-based speed measurement on highways, i.e. section control. The system functions in such a manner that a vehicle is photographed at point A of a section of road and the entry time is recorded, while at point B the exit time is recorded; on such basis the average speed for that part of the road is calculated. If such exceeds the speed limit allowed by law, an offence has been committed and an offence procedure is initiated against the owner of the vehicle. Such speed measurement can be carried out in a privacy-friendly manner – or not. The latter can involve massive monitoring of drivers and the creation of a large centralised data file, data processing – also with regard to drivers who have not committed an offence, excessive data retention, and similar. Taking into account the privacy by design concept, interferences with privacy can be minimised while all the objectives can still be achieved. With regard to the case presented here, the privacy by design concept envisages the following:

- photographing vehicles from behind;
- automatic transformation of the license plate number into the so-called DNA of the vehicle by means of one-way hashing algorithms, i.e. the creation of pseudonyms;
- measures preventing unauthorised access and data processing over the entire life cycle of data processing (from speed measurement to the communication of data to offence authorities);
- immediate erasure of entry data without matching exit data at point B;
- immediate erasure of data related to instances in which the speed limit was not exceeded;
- a minimal retention period regarding entry data without matching exit data (e.g. a few hours).

7. Respect for individuals

The design of solutions should also take into account the perspective of the individual and enable such to be appropriately informed regarding personal data processing, as well as simple default privacy settings, and similar. Solutions which hide information regarding personal data processing within illegible privacy policies and within complicated settings that are too technologically oriented, such that common users cannot understand them, do not satisfy the requirements of the privacy by design concept.

The privacy by design concept is the basis for these Guidelines regarding the development of information solutions, which are presented in more detail below.



Privacy by design and guidelines for the development of information solutions

Minimisation

In the initial phases of a project (when the desired functionalities are being determined), the minimum sufficient set of personal data with which the purpose of the processing can be fulfilled must be determined.

- If certain personal data are not needed, such should not be collected (what often suffices for achieving a set objective is anonymised or statistical data).
- If personal data are necessary, the principle of proportionality must be respected.

A practical example – e-ticketing in public transport

With regard to the use of monthly travel passes, is it necessary to process personal data regarding the location and time passengers enter public transport vehicles?

- In order to manage traffic flow or determine how busy individual lines and vehicles are, as well as for other statistical and analytical purposes, personal data, as a general rule, are not necessary as only anonymised data that can not be linked with an identifiable individual suffice to achieve the goals and as such may be processed!
- If the purpose is to monitor public transport users and offer them certain services according to their particular trips or routes (e.g. discounts, customised advertisements and offers, and similar), a proportionate set of personal data may be processed, however the legal basis for such (personal consent of the individual) is necessary!

Attention must be devoted to the fact that different purposes require a different scope of personal data, which is why it is incorrect to determine only one scope of personal data (usually the entire amount of all relevant extents of personal data) and generalise it for all purposes!

Proportionality

If it has been established that certain kinds of personal data must be processed, the following guidelines regarding proportionality must be followed:

- **Use less sensitive data rather than more sensitive data**

If you can choose, use non-descriptive identifiers (e.g. a series of numbers, the results of one-way hashing algorithms, and similar) rather than descriptive ones (e.g. a unique personal identification number that also reveals the person's date of birth and sex). Similar holds true for categories of personal data – wherever possible "ordinary" personal data should be used instead of sensitive personal data.

- **Do not collect multiple unique identifiers unless absolutely necessary**

- **Use the "hit / no-hit" principle wherever possible.**

Often there is no actual need to show among the results input data or other data that is of no interest to users.

- **Use pseudonyms rather than "raw" personal data.**

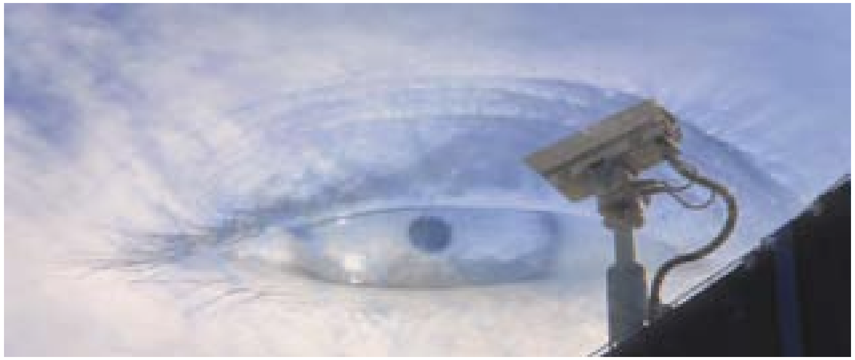
PLEASE NOTE – The risk of personal data being abused is reduced by means of pseudonyms, therefore the Information Commissioner recommends the use of such; however, pseudonyms must, as a general rule, be treated as personal data when they are used in relation to identified or identifiable individuals; the results of one-way hashing algorithms are also categorised as pseudonyms.

Proportionality must be ensured in all phases (privacy by design), also with regard to the following:

- **the design of search engines (what are the possible search criteria, what should appear as the result of a search) – a greater amount of data on the screen entails greater requirements regarding the traceability of different data access events;**
- **user rights (whether a certain user really needs access to certain data – a level-based approach) – a greater amount of data entails greater requirements regarding traceability;**

ACCESSING PERSONAL DATA

INCORRECT: Everyone, all data, always, without a trace!
CORRECT: a minimal set of data, appropriate access rights, traceable!



Individuals' control of their personal data

In the 1970s Dr. Alan Westin defined privacy as individuals' right to control, edit, manage, and delete information about themselves and to decide when, how, and to what extent information is communicated to others. In the information society, individuals unfortunately often encounter problems in the exercise of the above mentioned postulates and do not know who will process their data, to whom such will be communicated, and for what purposes it will be used.

In many instances, such objectives can also be met by means of personal data processing methods which envisage the retention and/or processing of personal data by individuals. A classic example of such processing is the future system of electronic tolling, which is to be based on paying tolls in accordance with the distance driven. In privacy-friendly solutions the raw data regarding the distances covered by individual vehicles are controlled by individuals; as described in the box, similar solutions exist with regard to biometric measures. It would be an illusion to claim that such trends regarding processing power in the direction of users does not entail financial consequences; however, what must be taken into account in the assessment of financial consequences are the costs that could arise due to personal data abuse. Such can be extremely high and could increase with the number of individuals whose data are being processed, especially as it is only a matter of time before mandatory data breach notification becomes obligatory for all data controllers. With this "trend" regarding data being under the control of the individuals concerned, risk and potential liability can be avoided.

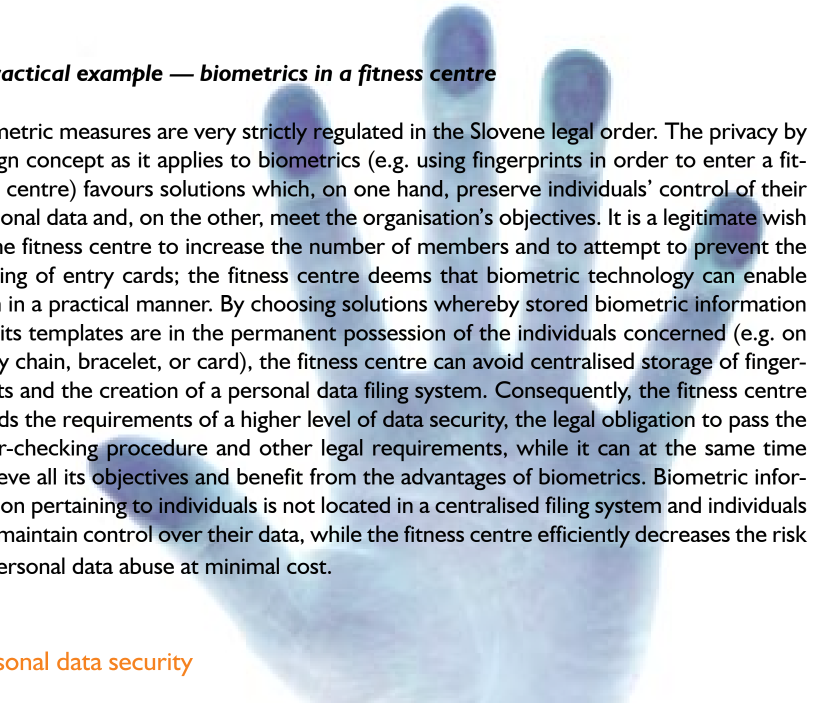
If processing data by the individuals concerned is not reasonable in certain instances, individuals can still be enabled control over their personal data by being offered the possibility to electronically access their own personal data, to export such personal data, and to use similar tools.

Please note – individuals are only entitled to their own personal data and not to data regarding specific persons who have accessed their data ("who watched me"). The lawfulness of such access can be examined by a state supervisor for personal data protection who is authorised to access such data.

The realisation of the right to self-determination is, naturally, pointless if prior to that one is not appropriately informed regarding personal data processing. What is referred to here, above all, are the privacy policies of websites which in their current forms are completely illegible to final users and do not meet the objective for which they were created. It is essential to provide users with answers to the following questions:

- Which data will be processed?
- Who will process the data?
- For what purpose?
- Will the data be communicated to third persons, and if so, to whom?
- How long will the data be retained?
- How can one learn about the data retained?
- How can one delete one's personal data from databases?

Such information can be presented to individuals in a brief, understandable, and easily accessible manner, possibly by separating such from the legal conditions for use. See also: The Guidelines of the Information Commissioner for Designing Website Privacy Policies



A practical example — biometrics in a fitness centre

Biometric measures are very strictly regulated in the Slovene legal order. The privacy by design concept as it applies to biometrics (e.g. using fingerprints in order to enter a fitness centre) favours solutions which, on one hand, preserve individuals' control of their personal data and, on the other, meet the organisation's objectives. It is a legitimate wish of the fitness centre to increase the number of members and to attempt to prevent the lending of entry cards; the fitness centre deems that biometric technology can enable such in a practical manner. By choosing solutions whereby stored biometric information and its templates are in the permanent possession of the individuals concerned (e.g. on a key chain, bracelet, or card), the fitness centre can avoid centralised storage of fingerprints and the creation of a personal data filing system. Consequently, the fitness centre avoids the requirements of a higher level of data security, the legal obligation to pass the prior-checking procedure and other legal requirements, while it can at the same time achieve all its objectives and benefit from the advantages of biometrics. Biometric information pertaining to individuals is not located in a centralised filing system and individuals can maintain control over their data, while the fitness centre efficiently decreases the risk of personal data abuse at minimal cost.

Personal data security

Personal data security is such a broad topic that a detailed description thereof would be beyond the scope of the present guidelines, therefore below we will only focus on some of the most exposed elements of personal data security, such as access rights and traceability.

In general, however, the Information Commissioner recommends following international information security standards, such as those that are part of the ISO/IEC 27000 family of standards; the Information Commissioner would like to call special attention to the fact that information and personal data security entails the implementation of not only technical but also (or perhaps even primarily) organisational measures, such as user education, internal and external control, the adoption and implementation of security policies, and similar.

Security measures must be appropriate with regard to the nature of the data processing and the risks that such entails. To illustrate the above-mentioned, a hairdressing salon and a major medical centre differ drastically with regard to the scope and nature of the personal data they control, as well as regarding the threats thereto. Thus, the security measures must differ appropriately.

What is extremely important for such is a risk analysis, the result of which is the main input data for the adoption of risk-mitigation measures. Unfortunately, the Information Commissioner often finds that in practice many companies and public administration authorities do not carry out even the most essential phase, which is a prerequisite for an appropriate level of security, entailing an analysis of the actual situation in terms of the following: which personal data they possess, what their information sources and means are, and similar. If one does not even know what personal data one has, one certainly cannot protect such appropriately.

The Information Commissioner would especially like to call the attention of information solution developers to the use of established cryptographic methods by means of which the integrity and confidentiality of data can be ensured. Cryptographic methods have broad application, encompassing everything from the safe retention of encrypted data, the transmission of data rendered illegible, the use of the same data for different purposes by means of cryptographic transformations which are not mutually linkable, to ensuring the unchangeability of data.

Due to possible exploitation of the vulnerabilities of computer systems resulting in partial or entire exposure of personal data nullifying all efforts invested in ensuring privacy, the Information Commissioner emphasises the importance of promptly and continuously detecting and eliminating such flaws. Furthermore, it is of special importance that periodically checking for known and frequently exploited flaws be integrated into the upgrading and maintenance cycles of computer systems that process personal data in any manner.

Access rights

The access rights of users must be clear and consistent with the tasks they carry out. The management of such rights must be up-to-date (in terms of granting, changing, and cancelling them), hierarchical, and documented. The use of shared access rights must be prohibited as it disables subsequent determination with regard to who has accessed personal data and when and which data was accessed or processed. Furthermore, what must also be explicitly prohibited is lending means of authenticating and authorising users, such as usernames, passwords, cards, and similar, except when such is absolutely necessary in exceptional cases.

Access logging

Data controllers are obliged to ensure the appropriate security of the data they process . In accordance with the requirements of the PDPA-1, the traceability of personal data processing refers to the broad term “processing of personal data”, which, according to the definition determined in Par. 3, Art. 6 of the PDPA-1, entails any operation or set of operations performed in connection with personal data that are subject to automated processing or which in manual processing are part of a filing system or which are intended for inclusion in a filing system, such as, in particular, collection, acquisition, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, communication, dissemination or otherwise making available, alignment or connecting, blocking, anonymising, erasure or destruction; processing may be performed manually or by using automated technology (the means of processing). In other words, such entails that with regard to the nature of the data that is to be processed and the risks connected to such, a complete audit trail must be ensured, which entails recording every instance of data being accessed. Deviations from this principle are possible only on the basis of appropriate risk analysis and management.

Access logging must be such that it enables subsequent checking as to who accessed the personal data, when such occurred, and which personal data was accessed; the identification of the persons who were in contact with the data must be unique, i.e. it must refer to a specific individual person.

With regard to such, special attention must be devoted to two important (and interrelated) issues – who controls the controllers and the authenticity and integrity of audit trails. The issue of who controls the controllers is related primarily to the issue of the competences of system administrators. The audit trail of personal data processing must be authentic and its integrity ensured, therefore appropriate technical and organisational measures must be ensured which implement control over the actions of system administrators. Systems must function in such a manner that it is not possible to temporarily turn off the system of access logging, even the highest level administrators, i.e. system administrators, must not be given the opportunity to subsequently correct, alter, or delete parts of or entire audit trails. With regard to such, it is reasonable to apply such implementation possibilities that ensure the non-repudiation, authenticity, and integrity of audit trails by means of methods such as the following: dislocated storage of audit trails (at locations which can not be accessed by the persons whose activities are recorded), the "four eyes" system, unerasable storage of audit trails , and the storage of data on accessing audit trails. No one is allowed to have uncontrolled opportunity to correct audit trails related to their activities or the activities of others, or the opportunity to temporarily or permanently "turn off" without control the recording of data in audit trails.

The traceability of personal data processing events refers to internal as well as external traceability. Internal traceability of data processing is defined in the above-mentioned Art. 24 of the PDPA-1, while external traceability, i.e. transmission traceability, follows from Par. 3, Art. 22 of the PDPA-1, which determines that for every personal data transmission event, data controllers must ensure that it is subsequently possible to establish what personal data was transmitted, to whom, when, and on what basis, for the period for which statutory protection of the rights of an individual due to impermissible personal data transmission is provided.

Requirements regarding traceability are lower if one strictly respects the principle of proportionality! This should be kept in mind in compiling queries, designing search engines (what the possible search criteria are, what will appear as the result of a search – a greater amount of data displayed on the screen entails greater requirements regarding the traceability of data access events), in designing the user interface (what is shown on individual screens, in individual tabs, and similar), and with regard to other elements of the information solution where it is possible to decrease the burden regarding ensuring traceability.

A practical example - logging

Such can be illustrated by the example of a user of a health care information system entering as his search criterion the name "Novak" and obtaining a list of a hundred patients and (some, not necessarily all) personal data pertaining to them. If - for example - the media published the information that a particular famous person is HIV positive, how can it subsequently be determined who leaked that information to the media (e.g. after learning of such information by searching in the system). Traceability can be ensured in two ways:
a) Such search instances are saved in an access log for every patient whose personal data were accessed. If this method is used, with regard to each individual it must be logged who searched for and accessed their personal data and when.
b) A repeated search must provide the same results, i.e. the result of a search at a certain time is logged. It must be logged who carried out the search and when, as well as what the result of the search was at that time.

Both methods are acceptable, but the decision of which one to use is left to the developers, who must take into account the aspects of functionality, available financial means, etc. In both instances it is of key importance to log who carried out each individual search, as it is only in such a manner that the liable person in the event of the abuse of personal data can be determined, which is the purpose of traceability.
If it is not possible to ensure the subsequent determination of which personal data were accessed by users (some or all), it is necessary to assume that by performing the search, the user has familiarised him or herself with all the personal data displayed and to enter such into the access log.

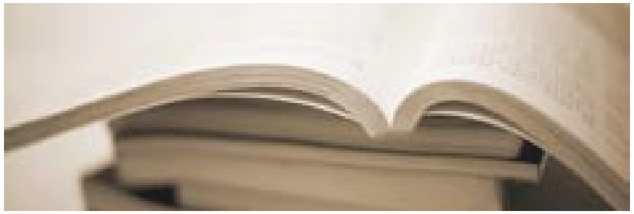
Retention period and the right to oblivion

The life cycle of personal data plays an important role in ensuring an individual's right to decide for him-/herself thereon. A special problem, especially on the Internet, is the implementation of the right to oblivion (i.e. the deletion of data) after the expiration of the purpose for which the data was used or after an individual has cancelled his/her consent to his/her data being processed. In France, the state encouraged the adoption of appropriate codes of conduct in order to ensure the right to oblivion in on-line social networks and in web browsers. The signatories of the code obliged themselves to appropriately inform individuals regarding whom they will entrust data to and for what purposes such will be used; such information is a basis on which individuals can freely decide whether to give consent to data processing and at the same time ensures them the right to refuse the processing of their personal data. Furthermore, the European Commission also announced that the implementation of the right to oblivion would be included in the amendments to the European directive on personal data protection.

In accordance with the provisions of Slovene legislation, personal data may be retained only for so long as is necessary to fulfil the purpose for which such were collected and processed. After the purpose of processing is fulfilled, personal data are deleted, destroyed, blocked, or anonymised . The data retention period must follow the purpose of the personal data processing, which is why it is recommended that such be determined in advance and that the principle of proportionality be respected with regard to such. The retention of data for possible future use is not permissible without well-founded arguments. In the event the retention period is not determined, it is recommended that individuals be informed of such.

Linking personal data filing systems within the public sector

Linking personal data filing systems from official records and public record books is regulated by the PDPA-1. With regard to the linking of personal data filing systems, the Information Commissioner calls attention to the fact that such linking must be determined by law and that, in the event any of the filing systems that are to be linked contain sensitive personal data (Par. 19, Art. 6 of the PDPA-1) or the use of the same linking element (unique personal identification number, health insurance number, or tax identification number) is needed to carry out linking, such linking is not permitted without the prior permission of the Information Commissioner. For more information regarding this, see the Guidelines of the Information Commissioner: Personal Data Protection with regard to the Linking of Personal Data Filing Systems within the Public Administration.



The most common mistakes

It is said that those who cannot remember the past are condemned to repeat it. In the experience of the Information Commissioner, the most common mistakes related to information solutions and personal data protection are the following:

SECURITY OF PERSONAL DATA

In the field of security of personal data, deviations from the established standards of information security cause the most problems. Information solution developers must pay attention to some of them, whereas certain measures (especially organisational) must be implemented by the users of such solutions. Such problems include the following:

- users' access rights are not determined;
- access rights are not suitable to the nature and requirements of the work;
- the existence of group rights (for example "team2");
- the means of authentication and authorisation are lent to others;
- the system does not ensure the traceability of personal data processing;
- traceability exists but data export events are not recorded;
- administrators can cover up traces of their actions;
- users do not abide by a clean-screen policy;
- sensitive personal data are sent via regular e-mail;
- traceability does not enable the person responsible to be traced;
- there is no separation of testing, training, and production environments;
- technical measures are ensured, but there is an absence of organisational measures (for example user education, internal control, and similar).

THE USE OF THE SAME LINKING ELEMENTS IN CERTAIN FIELDS

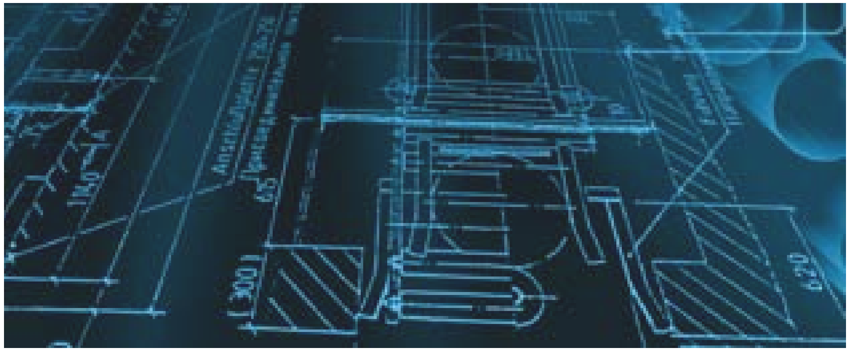
Using the same linking elements, i.e. unique identifiers, can be two-faceted with regard to personal data protection. On one hand, their use is problematic especially because such are ideal for linking several personal data filing systems, while they enable personal data harvesting. On the other hand, such can function as the guardians of one's data – just think about the amount of data one must sometimes supply when claiming a warranty, seeking help regarding the functioning of a product or a service, reporting damage to an insurance company, and similar, where the same linking element would be sufficient for one's identification, such as a buyer ID, the number of a subscription contract or policy, etc.

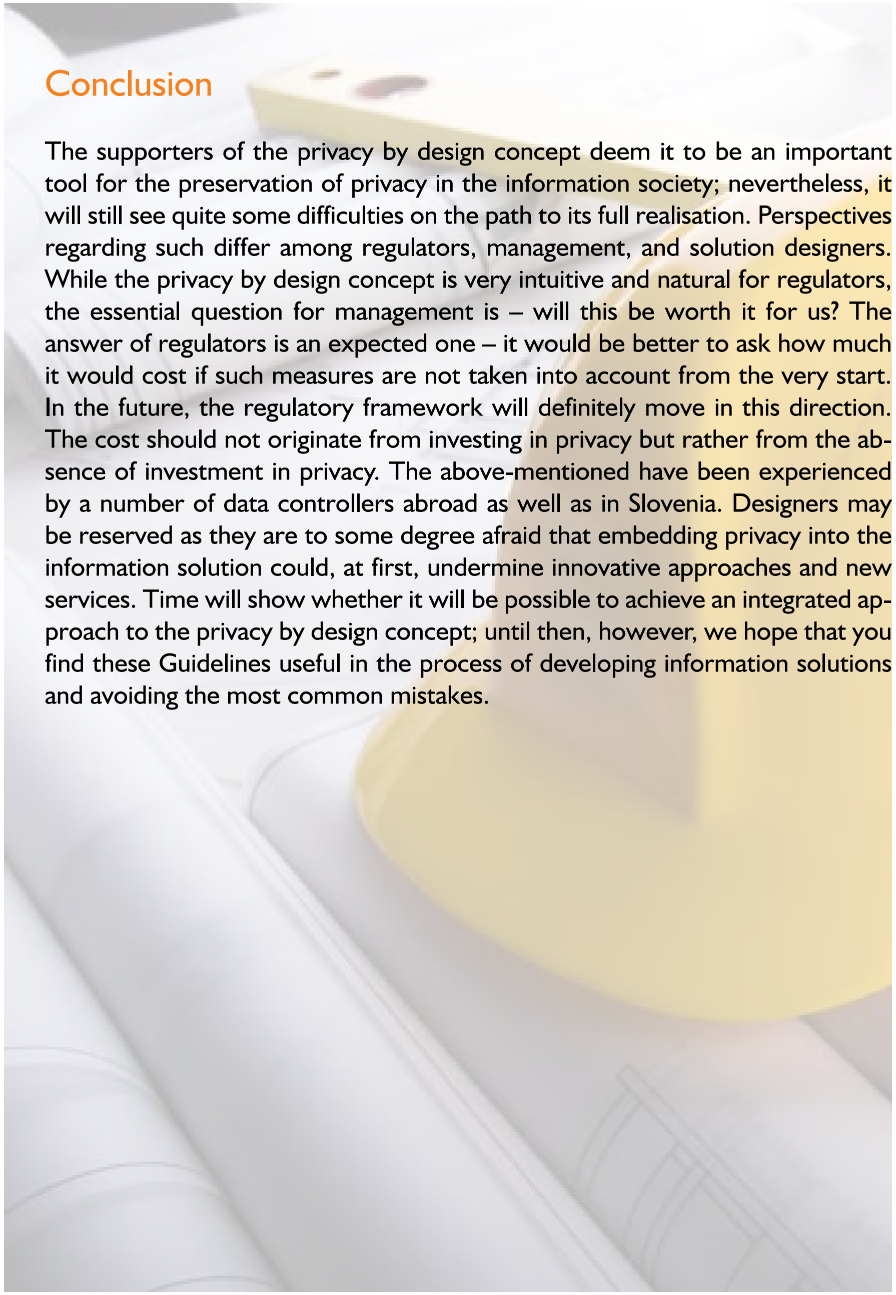
The PDPA-1 explicitly prohibits the use of same linking elements in such a manner that only such element would be used to obtain a piece of personal data (Art. 20 of the PDPA-1). The above-mentioned does not hold true for all data files but only for obtaining data from personal data filing systems related to the fields of health care, the police, the intelligence and security activities of the state, the judiciary and the State Prosecutor's office, and criminal and offence records. In other words, in these areas searching only by means of a unique personal identification number, tax identification number, or health insurance number is not allowed.

DISRESPECT FOR THE PRINCIPLES OF MINIMISATION AND PROPORTIONALITY

Symptoms which indicate disrespect for the principles of minimisation and proportionality are often reflected in statements such as "we need this, otherwise the system will not let you in"; in addition, the following mistakes are often made:

- data is collected although the system could effectively function without it;
- data that the data controller already has (regarding, for example, claiming warranties or insurance claims) is collected (again);
- data is collected for possible future use ("we might need it someday");
- several unique identifiers are required at the same time;
- retention periods are not determined or they are disproportionately long.





Conclusion

The supporters of the privacy by design concept deem it to be an important tool for the preservation of privacy in the information society; nevertheless, it will still see quite some difficulties on the path to its full realisation. Perspectives regarding such differ among regulators, management, and solution designers. While the privacy by design concept is very intuitive and natural for regulators, the essential question for management is – will this be worth it for us? The answer of regulators is an expected one – it would be better to ask how much it would cost if such measures are not taken into account from the very start. In the future, the regulatory framework will definitely move in this direction. The cost should not originate from investing in privacy but rather from the absence of investment in privacy. The above-mentioned have been experienced by a number of data controllers abroad as well as in Slovenia. Designers may be reserved as they are to some degree afraid that embedding privacy into the information solution could, at first, undermine innovative approaches and new services. Time will show whether it will be possible to achieve an integrated approach to the privacy by design concept; until then, however, we hope that you find these Guidelines useful in the process of developing information solutions and avoiding the most common mistakes.