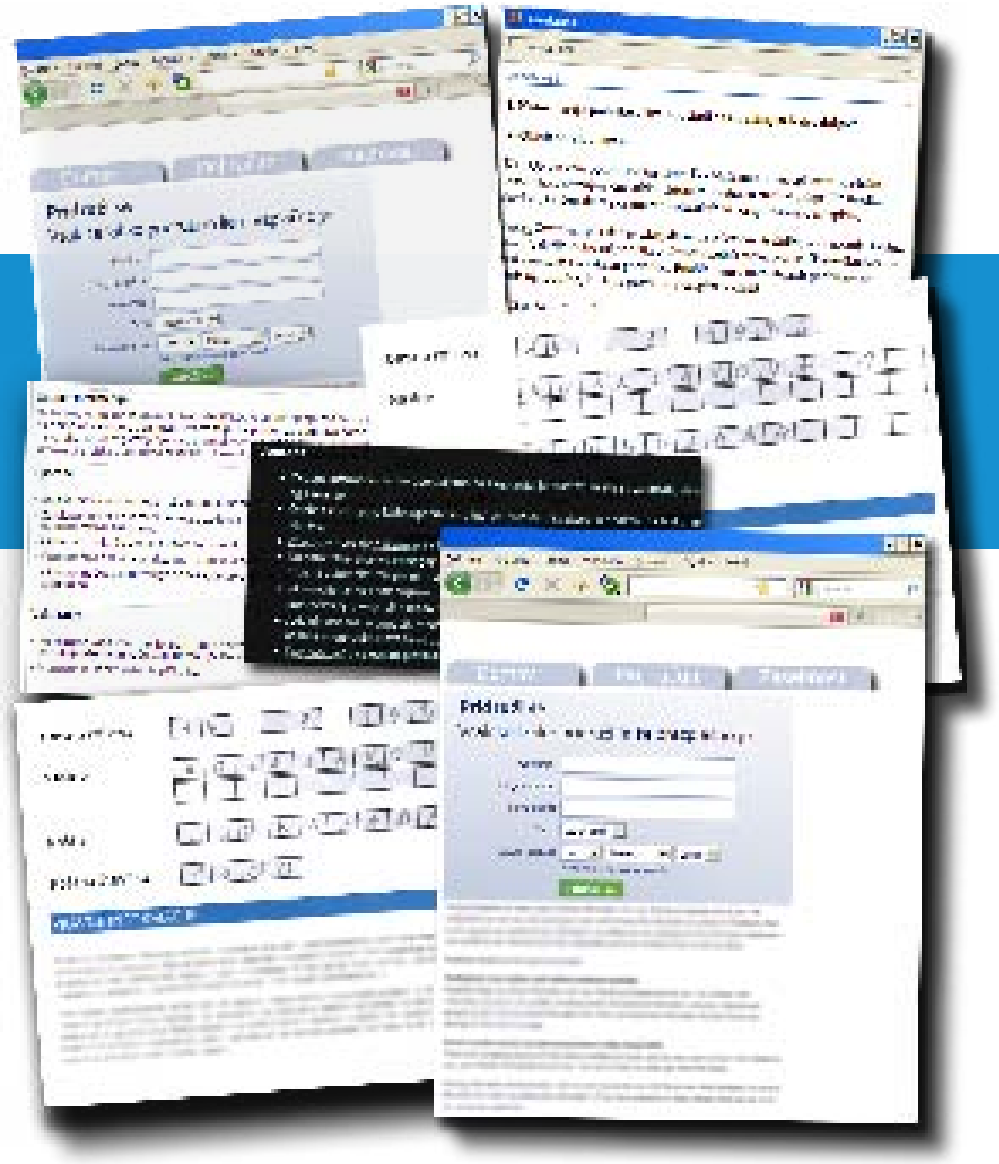
Code of conduct for personal data processing

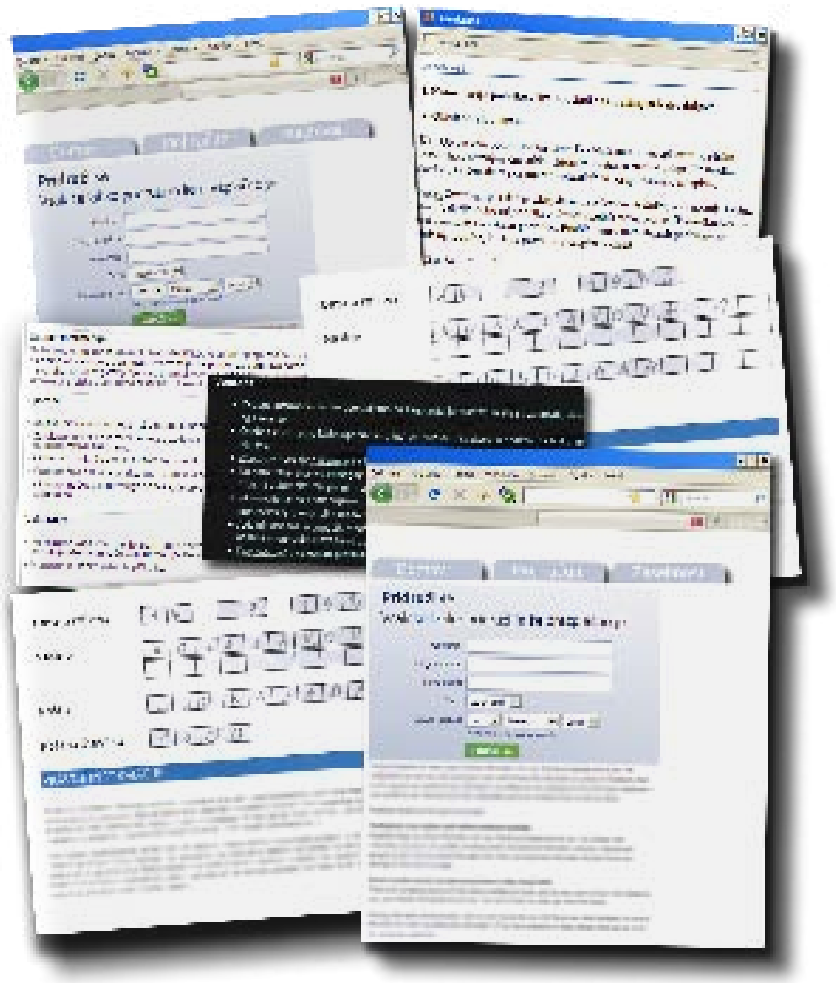
Guidelines for private sector



INFORMATION COMMISSIONER

Purpose of the document:	These guidelines provide answers to frequently asked questions by the providers of goods and services on how to deal with consumers' personal data. By examples of good and bad practice, the guidelines explain how personal data should be treated and processed in a lawful manner, and suggest recommendations for formulating the »Notice on personal data processing«.
Target groups:	Providers of goods and services; agencies conducting direct marketing and other marketing activities; contractual processors of personal data.
Status:	Public.
Version:	1.0
Published:	May 22, 2009
Authors:	Information Commissioner.
Key words:	Guidelines, providers of goods and services, marketers, personal data, personal consent, business practice, marketing, Notice on personal data processing, proportionality.

TABLE OF CONTENTS



About the guidelines

These guidelines have been prepared by the Information Commissioner (IC) as a practical and useful guide to be used by personal data controllers. They are written in a simple and clear way, in a form of frequently asked questions. Through the answers provided the data controllers will learn how to handle such data in an appropriate manner and compliant with the requirements of the Personal Data Protection Act (Official Gazette RS, No. 94/07 – official consolidated text; hereinafter: ZVOP-1).

The legal basis for publishing this text derives from Art. 49 of ZVOP-1, under which the Information Commissioner may prepare and issue non-binding instructions and recommendations regarding protection of personal data in individual fields and publicise the information on its website, or communicate such information in some other manner.

See also:

- *Opinions of the IC:*
  http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/

- *Brochures of the IC:*
  http://www.ip-rs.si/publikacije/prirocniki/

The Guidelines are also available at:

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

Introduction

The Information Commissioner's experience has shown that private sector organizations use different approaches in collecting personal data. These practices may vary significantly – from very transparent, fair and lawful methods, to examples where data subjects are not given complete information on how their personal data will be processed, are being cheated, or even forced to supply their personal data. .

Customers should be informed clearly and friendly about the purpose of personal data collecting and processing. . With these Guidelines the Information Commissioner instructs the private sector data controllers on how to treat their customers' data. As a rule of thumb, companies should try to put themselves in the shoes of data subjects who have been asked to disclose their personal data and answer the following questions:

- Will data subjects know **who** is collecting their personal data?
- Will data subject understand **the purpose of collecting** these data?
- Are data subjects aware of the **possible consequences of processing** their personal data?
- What if they object to **processing of their personal data and want to make a complaint**?

To avoid any possible complaints companies need to be aware that only properly informed individuals are able to give meaningful consent to processing of their personal data.

COLLECTING AND PROCESSING PERSONAL DATA: what data, how and from whom?

Q: When are we allowed to collect personal data and from whom?

Three basic conditions need to be met if you want to collect and further process personal data:

1. there should be a **legal basis** for the collection of personal data:

Personal data in the private sector can be processed if the processing of personal data and the personal data being processed **are provided by law**, or if **personal consent of data subjects** has been obtained for processing a particular personal data. If the law allows collection and processing of personal data, the purpose of processing of such data must be defined as well. If personal data are collected with the consent of data subjects, they must be **informed on the purpose of personal data processing beforehand, and if necessary, other information must be provided to ensure lawful and fair processing**.

Personal data processing is also allowed if a contract has been **concluded between an individual and a private sector subject**, or if a company, upon the initiative of individuals, is in the phase of **negotiations for concluding a contract**, provided that the processing of personal data is necessary and appropriate for negotiations to conclude a contract or for the fulfilment of the contract.

In addition to this, private sector entities may process personal data also if it is necessary in the lawful interests of the private sector and the interests clearly **outweigh the interests of the individual** to whom the personal data relate.

2. **purpose of processing** needs to be lawful and clearly defined.

3. **proportionality** of processing: providers of goods and services can only process the **data** which are **adequate and in their extent appropriate in relation to the purposes for which they are collected** and further processed (e.g. if you need to bill a customer you only need customer's address and not the information about the number of household members).

Q: Which data may be collected from data subjects?

There are three basic personal data protection principles you need to observe:

- fairness,
- lawfulness, and
- proportionality.

Fairness is a general requirement which demands a bona fide approach, i.e. you should not mislead your customers on how you process their personal data. Thus prior to the collection of data, personal data controllers need to obtain customers' personal consent and clearly indicate the purpose of collecting the data so as to eliminate any different interpretations. Do not lead your customers to believe that their personal data are going to be processed for one particular purpose only (e.g. sending bills for a service), while the data would be actually used for another purpose (e.g. direct marketing).

According to the principle of **lawfulness** personal data can be processed by private sector institutions if the processing of personal data and the data being processed has been **defined by a statute**, or if **personal consent of data subjects** has been obtained for such processing.

Providers of goods or services are allowed only to process the **data, necessary to fulfil the purpose of the contract with the customer**. This is the so called **proportionality principle** and it is one of the basic principles of personal data protection. For example, if a vendor receives an order for supplying goods to a customer, the only data necessary to complete the order is the customer's delivery address, and not his unique personal identification number, or some other personal data. If you request personal data from data subjects you need to be able to give a reasoned explanation why processing such data is necessary

for the achievement of a particular (lawful) aim. Disproportional or excessive collection of personal, data brings more risk for violations of privacy and abuse of personal data and requres more effort to ensure proper security.

Further below we present some examples of personal data which require particular considerations. These are: unique identifiers, as for example unique personal identification number (EMŠO), tax identification number, health insurance number, and sensitive personal data.

Unique personal identification number (EMŠO)

Processing of the unique personal identification number (EMŠO) is regulated by the Central Population Register Act of Slovenia, which stipulates that EMŠO is a **personal identification number** by which **individuals are uniquely identified.** Identification is necessary for administering and maintaining databases on population, for linking the data across the databases and for rationalising work of state bodies and other users, authorised by the law. **Persons collecting** EMŠO need to have a **legal basis for this and a defined purpose for collecting such information.** If you need to obtain a written consent from data subjects, you **need to inform them about the purpose of using this information!** Before requesting EMŠO you should always ask yourself whether the same purpose could be achieved by processing some other data, since EMŠO, belongs to the category of data which reveals additional information - the date of birth, sex and nationality.

In what cases are we allowed to ask for EMŠO?

- If a **written personal consent** has been obtained **and if data subjects have been informed about the purpose of processing**, or
- if **provided by law**;
  and
- if this is necessary for **achieving a legitimate purpose of processing.**

Tax identification number

Tax identification number is assigned to taxable persons and is used for tax purposes. The Commissioner notes that companies are allowed to collect tax identification numbers only when it has been unequivocally established that an individual and a company are entering a tax relationship, e.g. in games, when the recipient of the money prize needs to know how much to declare for personal income tax, or what amount the donor needs to deduct for taxes, according to the provisions of Personal Income Tax Act (Official Gazette RS, No. 117/06, hereinafter: ZDoh-2). Therefore, **processing tax identification number of individuals in advance, i.e. when it has not been clearly established yet that the individual and the company are entering a tax relationship, isn't compliant with the principle of proportionality**, which stipulates that personal data being processed must be adequate and in their extent appropriate in relation to the purposes for which they are collected and further processed.

Identity documents

Personal identity documents in Slovenia are the following: **identity card, passport, driving licence, or some other official document, issued by an appropriate authority. These documents must contain a photo of the citizen (e.g. firearm licence)**. Citizens of Slovenia are obliged to present their personal identity document to authorised persons. However, identity documents must not be given or lent to other persons, or pledged in order to protect one's benefits or rights. By logical interpretation, one could assume that **any photocopying of personal identity documents to protect the benefits or rights is prohibited as well**. It is clear that the original document and a photocopy are different in character, however, photocopies containing personal data of individuals can be abused as well.

Art. 3a of the Personal Identity Card Act (Official Gazette RS, No. 71/2008 – official consolidated text; hereinafter: ZOIzk) stipulates that data controllers are allowed to **copy personal identity documents only in cases provided by the statute.** Similarly, Art. 4a of the Travel Documents Act (Official Gazette RS No. 3/06 – official consolidated text and 44/08; ZPLD-1) stipulates that data controllers may copy **passports only in cases provided by the law**.
Only the **holder** of personal identity card or passport, and the **notaries** and **financial institutions**, performing financial services are allowed to photocopy

documents **if this is necessary for proving the identity of citizens in a proceeding.** Photocopying is also allowed if **a written personal consent has been obtained** from the holder of the identity card. In such case a photocopy needs to be suitably marked with a note that the copy of personal identity card or passport will not be used for any other purpose. **Any further photocopying of the copy is forbidden**. If the holder of such document requests so, the data controller is obliged to issue **a certificate of the copy** of the **personal identity card or passport**, where **the purpose of use of the copy** and **the period of use must be indicated.** Only the holder of personal identity card or passport may sign the photocopy. It is forbidden to keep copies of personal identity cards or passports in electronic format.

Q: When can we make a photocopy of a personal identity card or passport?

- If provided by the statute;
- Only the holder of the document, the notaries and financial institutions are allowed to photocopy personal documents;
- Upon written consent of the holder of the document.

For example, may hotel receptionists, mobile service operators, or shop assistants make a photocopy of a personal document? The answer is yes, if the holder of the document agrees to this, and if this is an act of free will.

Sensitivity of personal data

Sensitive personal data are data on racial, national or ethnic origin, political, religious or philosophical beliefs, trade-union membership, health status, sexual life, the entry in or removal from criminal record or records of minor offences that are kept on the basis of a statute that regulates minor offences. Sensitive personal data are also biometric characteristics by which it is possible to identify individuals in connection to any of the circumstances mentioned above.

Q: In what cases can we collect and further process sensitive personal data?

- **if the individual has given explicit personal consent to this. As a rule, the consent must be given in writing,**
- **if provided by the statute,**
- if processing is necessary to protect the life or body of an individual to whom the personal data relate,
- if they are processed for the purposes of carrying out lawful activities by institutions, societies, associations, religious communities, trade unions or other non-profit organisations with political, philosophical, religious or trade-union aim,
- if the individual has made them public,
- for the purposes of protecting the health of the public,
- if this is necessary in order to assert or oppose a legal claim.

Q: How to obtain personal consent from individuals and in what form?

As already said, to make the collection and processing of sensitive personal data legal, it is necessary to obtain personal consent from data subjects. Personal consent can be obtained in different ways and in different formats.

In any case, some **general provisions of the legislation in force** must be applied:

1. Personal consent needs is a **voluntary statement of the will of an individual.** Personal consent is considered involuntary if:
   - given under **threat** (by unlawful intimidation of consumers), by **fraud, or by misleading the consumer** (e.g. if a company persuades a consumer to give his e-mail address for sending bills but the information is in fact transferred to third persons for marketing purposes); the individual has been **blackmailed**;
   - **and if the data controller requires information which is not neces-**

sary for achieving the purpose (e.g. we are not going to extend the warranty for the product if you do not provide your UPIN). **Such provisions in a contract are deemed as unfair terms and are void!**

2. 2. Personal consent must be based on the **information** provided by the data controller, as stated in Art. 19 of ZVOP-1. The information must include the following:

- **Purpose** of processing personal data;
- **Who** is going to process the data (would it be the controller or its representative, in which case you need to give personal name, name of the company, and seat);
- **Other information if necessary to ensure lawful and fair processing.**

3. If you request a customer to sign a consent form, the form (as well as other conditions from the contract) is **binding for the customer only** if he/she has been **previously acquainted with the whole text of the form**. This means that customers must be explicitly warned, and the text needs to be easily accessible. The **text of the consent form needs to be clear and understandable**, since unclear provisions will be **interpreted to the benefit of the individual.**

Customers must be **well informed before making a decision**. Only in this way their consent can be considered as valid!

Consent can be given in one of the following forms:

a) Written consent: is a signed consent in the form of a document, provision of a contract, the provision of an order, an appendix to an application or other form in accordance with the statute;

b) Oral consent: is an explicit oral permission for data processing for a defined purpose; such consent can be given face-to-face or by means of telecommunications (however such consent is more difficult to prove in case of dispute);

c) some other appropriate consent of the individual: it can be given by telecommunication or some other appropriate means, but has to allow unambiguously conclusion that a consent has been given.

If your customer does not respond to your question whether he/she agrees with personal data processing, this does not mean implicit/silent consent! However, any action of an individual from which it **can be unambiguously concluded** that he/she agrees with data processing is deemed to be consent (see above – other appropriate consent). If there is a provision in the contract saying that silence or inactivity of the individual means that the consent has been given (e.g. if the customer has not turned down your offer within a certain time limit) such provision is void. Also, a consent obtained under pressure is void. It the customer has been **forced** to provide some personal data (e.g. for direct marketing purposes) on the basis »take it or leave it« this cannot be considered as an act of free will. If a person has been forced to provide some personal data in order to benefit a service, and if this data is unnecessary for performing the service, or if the individual has been given no choice, it is difficult to talk about voluntary statement of the will, and the »consent« obtained this way is considered inappropriate because the data controller had no legal grounds for processing personal data. The meaning of personal consent as a voluntary statement of the will is even more relevant if the consent has been obtained by force and when personal data has been made available to several direct marketers (who are frequently unidentified)

Personal consent from minors

Personal Data Protection Act does not specify the method for giving personal consent (oral or written), when the data subjects are underage children (minors). Therefore, in such cases it is necessary to apply the general provisions of the Law of obligations and the Family law. These regulations refer to the capacity of persons to conclude »legal transactions« and »contracts«. Consent to processing of personal data may be treated as belonging to the same category.

1. Children above the age 15:

When you are dealing with children above the age 15, you will need **parent's approval** to make your legal transactions valid:

- if transactions are **such that might significantly interfere with adolescent's life,** or,
- if transactions are such that they could have **impacts on adolescent's life even beyond their age of majority**.

In the the Commissioner's view, processing of personal data for the purpose of play contests does not reach such level of »importance« as to require parental consent. In this case the capacity of an individual to contract will suffice. However, in certain cases, depending on how a particular service is carried out, and on the consequences of processing personal data, this will not hold.

2. Children under age 15:
Children under age 15 are considered as completely incapable natural persons in terms of handling business activities and therefore **they alone can not express business intentions**. For this reason they need parents or a legal representative to express this intention on their behalf. In judicial practice, a contract, concluded with a person incapable of making business transactions is void (in theory even non-existent). By analogy, giving consent to processing personal data (as a legal act) is deemed to be void too. Therefore, you need to be aware **that children under age 15 are incapable to understand the meaning of giving consent and possible consequences of giving such consent.** For this reason **their parents, or legal representatives, need to act on their behalf.**

Asking for parent's consent by **electronic communication means is questionable since it would be difficult to implement it in practice.** It would be impossible to establish whether it was the parent or the guardian who gave consent to processing the data (it is also impossible to identify the age of children). Thus the data controller should find a technically suitable method for obtaining parents' consent with regard to the specific character of the offer.

Transferring personal data to third persons

If you wish to transfer personal data to third persons, the **data subjects must consent to this.** The data subjects must be informed about **which data** are going to be transferred, **to whom** and for **what purpose**. Data controllers in the private sector need to be aware that selling, renting, supplying, or any other similar handling of personal data, such as keeping customer databases, register of clients, etc. are **illegal** without data subject's consent! As already said, a precondition for obtaining personal consent is that individuals are precisely informed about the person(s) who are going to process their data and about the purpose of use.

Obtaining consent is not necessary in the so called **contractual processing**. Your **contractual data processor** that will perform certain activities which involve personal data processing, **in your name** and on **your behalf** e.g. carrying out surveys on your behalf, or other forms of direct marketing, is not obliged to obtain approvals from individuals but it is your duty to obtain such consent.

When supplying personal data to your contractual partners you need to make sure that they are clearly aware **which** data they are authorised to use, **what is the purpose of their use** and what they are allowed to do. Such **authorisation** must be precisely defined in a written contract, while the entire process of contractual processing needs to be carried out in compliance with the provisions of Art. 11(contractual processing), and Art. 24 (security of personal data) of ZVOP-1.

"NOTICE on DATA PROCESSING " AND PERSONAL CONSENT

The main legal obligation of the private sector is to obtain personal consent in a fair and legal way. This is especially important should violations during personal data processing occur, for identifying responsibility. Consent to processing data for a particular purpose is considered as **a voluntary statement of the will** only if the data subject knows which data will be processed, for what purpose, and who will be using the data.
Further below you may find suggestions on **how to formulate Notice on Data Processing**, based on which individuals will be able to decide whether or not to give consent to processing of their personal data. The text should be written in a clear and understandable manner.

What is Notice on Data Processing?

Notice on Data Processing (hereinafter: the Notice) is a written or oral statement which contains the following information:

- what is the intention behind collecting and processing personal data,
- what data are going to be collected,
- who will collect the data,
- the purpose of collecting.

The Notice may also contain other pieces of information, e.g. possible adjustments of data protection.

The main purpose of the Notice is to give assurance that personal data will be collected and processed **in a fair and lawful manner**. For this reason, the notice needs to be **transparent** and **informative, helping individuals to clearly understand** how their data are going to be used and **what could possible consequences of such use be**. Remember, **you will gain trust of your customers only** if they have been correctly informed.

Formulating the text of the Notice

Through the process of writing the text, try to reflect on the questions: is the data I am requesting **really necessary**, and **what** is **the purpose of processing this data?**

The main purpose of the Notice is to inform your consumers, therefore the text must be written in a clear and understandable way.

Is the Notice clear enough?

To test whether the text of the Notice is clear and understandable enough for an average person, try to ask yourself if the reader would understand:

- Who is collecting my personal data?
- What is the purpose of collecting?
- What are possible consequences of collecting and processing?

An example of clear Notice:

What: If you want to subscribe to our E-newsletter we need your e-mail address. Please enter your mail address in the box provided.

Why: Your data will be processed exclusively for the purpose of informing you on the news in the filed of your interest.

How long: You e-mail address will be kept in the database until you decide to unsubscribe and stop receiving the news. You can unsubscribe any time. When you receive our e-mail click unsubscribe, or visit our web site here.

Are my personal data going to be made available to third persons? NO.

An example of unclear Notice:

The Company Ltd. collects and processes personal data of individuals in compliance with the law governing personal data protection, i.e. Personal Data Protection Act (Official Gazette RS, No. 94/2007, official consolidated text), which gives legal basis for processing personal data, security of personal data and obtaining personal consent of individuals for transferring the data to third persons.
With personal consent of individuals the Company Ltd. is allowed to use personal data from Section A of the questionnaire for performing marketing activities by different advertisers…

It is also important what terminology you are going to use in the text. Avoid any wording difficult to understand for an average consumer, and avoid technical terminology used in the language of law.

Remember, the consumers must be absolutely sure that they understand the meaning of the text which precedes the statement "I accept and agree with the conditions of my personal data processing".

The Commissioner recommends a **layered** text of the Notice. The best way is to prepare a simple and clear **summary of the key messages** you want to convey to the users. Provide hyperlinks within the text which will lead the reader to the whole text as necessary. This way your text will be a user-friendly interface between your summary and the entire text. In any case, make sure the summary contains all the basic information: who is collecting the information, what data are being collected and for what purpose.

Example:

Summary:
If you tick the box below and press »Submit« you will:
- start receiving our advertisements and news;
- start receiving our advertisements and news from other companies;
- You will receive maximum one message per week;
- If you unsubscribe you will stop receiving all mail from us.

Please read detailed conditions of our company advertising policy here.

Whole text:

Our company is engaged in direct marketing and would like to process your personal information in order to send you advertising material. If we receive your consent for direct marketing we will start sending you our publicity information. If we obtain your consent we are going to collect and further process you e-mail address which you need to provide in the form. You will also receive advertisements from other companies. Your e-mail address will be kept in the database until you decide to unregister. You can stop receiving e-news any time by clicking on the link, or you can unsubscribe from our web site. When you fill in the registration you need to indicate that you agree that you mail address be used for informing you on the news and that you understand that you can unsubscribe any time you want by clicking on the link in the e-mail message, or directly from our web site.

Remember! If you communicate the message clearly and the customers know what data you are collecting and how they are going to be treated, they will feel comfortable and trust you. In the opposite case, if your message is blurred and involves sensitive personal data you may soon expect complaints.

Transparency of your intentions is of utmost importance when personal data are in question. Your customers need to know they have a choice whether or not to make their personal data available and how they can prevent processing of their data.

What is the difference between the Notice on Data Processing, privacy policy and personal consent of individuals?

ZVOP-1 does not explicitly prescribe privacy policies, however, it provides a list of the information that data controllers need to communicate to data subjects. Thus, the Notice is the compulsory information which needs to be provided, while privacy policy is a broader concept and involves other aspects of personal data protection relevant to data subjects, e.g.:

- **will personal data be transferred and to whom**, how they are going to be processed and for how long the data will be kept;

- **for how long will personal data be retained;**
- which pieces of information are **obligatory** (e.g. is mobile phone number an obligatory or optional item);
- what are the **preventive measures** to avoid the abuse of data;
- **how can data subjects exercise their rights** (according to Art. 73 of ZVOP-1 informing the data subjects about their rights in direct marketing is obligatory);
- **who should they contact** for further information or in case of complaints.

A clear and transparent privacy policy is an example of good practice. If you want to gain trust from your customers, make sure that your customers are well informed: do not give only the compulsory information required by law but provide broader information as well.

What is the difference between the **Notice and personal consent?** The Notice is a way of informing the customers on how their personal data will be processed, while personal consent means an explicit declaration given by data holders by which they express agreement (and give consent) to processing of their personal data (see the example below). The most appropriate way of formulating the consent is: » I understand and agree with …«, where the consumer must **actively check the box.**

Example:

NOTICE
Your personal data will be collected and processed according to the provisions of the statute governing the protection personal data. Without your prior and explicit consent your data will not be disclosed to third persons.

CONSENT
☐ I understand and agree to the terms and conditions for receiving your notifications and special offers.

In some cases customers are obliged to provide personal data by law, therefore in such cases it is not necessary to ask for personal consent. You are expected only to provide a clear notice saying that giving personal data is required by law.

Methods of providing the Notice

The Notice can be provided:
- orally (e.g. by telephone, in person),
- in writing (printed announcements, SMS/MMS messages, via web sites, electronic mail, forms, etc.),
- by warning signs (e.g. these premises are under video surveillance)

To inform the consumers about the intended data processing we recommend you to use the **same medium as you have used in collecting the data**. Thus, if you have collected personal data via SMS messages, use the same channel further on for sending the Notice and obtaining the consent. Try to avoid using mixed media, e.g. do not collect personal data from questionnaires which you have published in paper media (newspapers), and post the Notice on the web site.

Providing the Notice to vulnerable consumer groups

When you collect data from vulnerable groups of consumers (e.g. children), consider proper formulation of the text. The message in your Notice needs to be clear and understandable to every young person you collect data from. If you collect data from persons with limited business capacity (children of age 15-18), the text needs to be suitably adapted.

If you engage in web marketing for children it is difficult to assess the real age of the data subject. Therefore, you need to ensure suitable security measures for the parents to prevent their children from providing personal data when interacting directly with your company.

Update your Notice

The Notice is a part of the contract between you and the customer and is therefore binding. Make sure that the notice does not contain any old-dated or incorrect information.

A useful method to verify the efficiency of your Notice is to analyze the complaints you have received from your customers about privacy issues. If your customers claim that your Notice is misleading, or difficult to find, you should

reformulate the notice, or move it to another, more visible place.

Four golden rules for collecting personal data online

The internet has become the most popular medium of modern information society where enormous amounts of data are being processed. The main question is how to collect personal data in a fair and lawful manner? For website publishers collecting data for the purposes such as play contests, direct marketing or other, the Commissioner's advice is to adhere to the following recommendations:

1. Keep your visitors informed in a clear, easily accessible and transparent way (see the example below) and explain what is the **purpose of collecting** and further **processing of their personal data** and what are their **rights**.

What data do we need from you?
Please give us your **contact information** (name, surname, e-mail address). We will need this for the purposes stated in the first three indents in the text above. If you wish to receive information by ordinary mail, please give us your **home address**.
We can only conclude contracts with adult persons. Therefore we also need your **date of birth**.

We need your data:
- to contact you should problems arise with the contract;
- to let you know about possible changes (tariff, etc.);
- to send you weekly updates on our offers;
- to verify if you are an adult and thus liable to conclude a contract with us.

2. If you decide to use tick boxes, leave them empty by default. If you are involved in direct electronic marketing, use the opt-in principle (prior consent), which requires the user to consent to data processing by clicking the box)

CORRECT:

If you would like to receive our newsletter, please check the box below and press »Submit«

☐ I give permission to the Company Ltd to send me notifications and special offers to my e-mail address given above.

INCORRECT:

☑ I give permission to the Company Ltd to send me notificatios and special offers to the e-mail address given above.

3. If you collect personal data from individuals **for different purposes**, or if the information is going to be used by external data controllers , and if you decide to use tick boxes , you need to provide a list of tick boxes to allow the users to express their choice.

☐ I give permission to the Company Ltd. To use my e-mail for **sending me information on the changes of** general terms;

☐ I give permission to the Company Ltd. **to send me announcements and special offers** to my e-mail given above.

☐ I give permission to the Company Ltd. to give my e-mail address to third persons for advertising purposes. I understand and agree wit the conditions of advertising of third persons. Read the conditions here.

4. If possible use the so called double opt-in. This means you send an e-mail to the address you have received and ask the recipient to reply to it. By replying to the message (or by clicking on a link) Tthe subscriber will confirm that he/she indeed is the same person that entered the e-mail. (See the example below). This eliminates the chance of abuse where someone submits somebody else's email address without his knowledge and against his will.

We add names to our list only after we have verified the recipient's permission, which is why we are sending you confirmation request to this address. To confirm and activate your registration, please click here.

From: Company Ltd. <online@podjetje.si>
To: janez.novak@elektronskaposta.si
Date: 23. 5. 2009
Ref: Registration online

Dear customer,

To confirm your online registration, please click here.

Best regards,

Company Ltd.

CONCLUSION

Personal data processing usually begins with the collection of data. . It is important that data controllers comply with the principle of lawfulness and fairness. As a rule, the private sector needs to obtain personal consent from data subjects to process their data. A meaningful consent can only be given if the users have been able to actively and freely express their will to entrust their data to a data controller for further processing. Unfortunately, experience shows that processing of personal data in the private sector is frequently not transparent, misleading and unlawful.

Hopefully, data controllers form the private sector will find these Guidelines useful. We hope that good and bad practice examples presented here offer valuable advice on how to ensure collection of personal data is carried out in a lawful manner and compliant to ZVOP-1. Private sector organizations, who collect personal data in a fair and lawful manner, who communicate information to their customers transparently and comply with the principle of proportionality, will, on a long run, gain confidence of their clients, and by appropriate handling of data, also avoid any violations of ZVOP-1.