The Principles of Work with Personal Data Pursuant to the Personal Data Processing Guidelines

İnsana Değer Derneği

Introduction

The purpose of the Guidelines on the Processing of Personal Data is that all IDD employees should start considering the impact of any personal data collection and work with data more carefully. And the objective is that requirements arising from the **GDPR** (General Data Protection Regulation) be complied within the course of workingwith personal data in IDD.

Scope of application

The principles apply in full to all full and part-time employees, volunteers, interns, consultants and trainees, as well as any other persons if they represent or act on behalf of IDD (hereinafter referred to as “Employees”).

The rules embodied in these Principles set the minimum standard. Individual departments may apply stricter rules which must, however, be based on these minimum standards.

General terms

What is personal data:

Any data on the basis of which a specific individual (data subject) can be identified: from electronic data, such as an e-mail address, IP address, or cookies to more typical data such as a name, address, and personal identification number, to sensitive data, for example, about one’s state of health or ethnicity. Personal data also includes photographs and audio/video recordings.

Data collection:

Essentially, data can be obtained in two ways – directly from data subjects or by other means (from publicly available sources, such as the Internet, by purchasing a database from a company, etc.).

In both cases, we are obliged to inform the data subject that IDD has obtained this data (and from what source, if applicable), state IDD’s basic contact details, state what data IDD has obtained, what it intends to do with it, how long the data will be in its possession, what legal grounds there are (see below), whether (and to whom) it intends to transfer the data, and tell him/her about the about basic rights of data subjects.

The difference is in that when obtaining data directly from the subject, we must inform the subject at the time of collecting the data, whereas otherwise, it suffices to inform him/her within one month of having collected the data.

When processing personal data of underage children, the age limit of 15 years is decisive – in the case of smaller children, the child’s legal guardian (most frequently a parent) must be informed (i.e. grant consent).

Typical examples of obtaining personal data: the completion of an online form, a subscription to a newsletter, obtaining data from newly recruited employees, the filling in of an attendance list, obtaining data from a client while working with him/her, etc.

As soon as IDD obtains data, it becomes the controller with respect to that data (and in some cases, IDD is also a processor if it works with the data for the purposes and in line with the instructions of another person); in both cases, it has a number of obligations when handling this personal data.

The main things you should consider before you start working with personal data:

- Whether it is indeed personal data;
- How we will collect it and how we will check that it is correct (and that it is being provided to us by the authorised person);
- What we need / want it for (that is the basis of the legal grounds for working with the data, see below);
- To what extent we need it (the extent should be minimised);

- For how long we intend to use the data (the length of time should also be minimised); Who will work with the data (who will have access to it);
- Where it is to be stored and how it will be protected from unauthorised use (this includes saving it on a computer or in the cloud, as well as the place where you store documents on paper, whether you are not allowed to leave them lying around in a printer, whether your mobile is password- protected, etc.);
- Whether we will wish to transfer it to someone outside of IDD (or whether someone else is going to process it for IDD);
- What will happen to the data once the period for which we can use it expires (who monitors the length of time, who is responsible for deleting or rendering the data anonymous, how will it be technically executed).

What are the (most frequent) legal grounds for working with personal data:

- It is necessary for the performance of the contract to which the data subject is a contractual party; It is necessary for compliance with a legal obligation applicable to the controller (IDD);
- It is necessary for the legitimate interests of the controller or a third party;
- The data subject granted their consent to the processing of their personal data.

In the first three cases, we do not require the data subject's consent, we only inform him/her.

In the last case, we need for the data subject to grant us their consent to the processing. The consent must be free (i.e., the subject can, but is under no obligation to grant it, or may withdraw it at a later point without this having any impact on the provision of services to the subject), informed (the subject must know what he/she is agreeing to), and explicit (i.e., we want the subject to sign it, check it off on the web, etc.).

PRINCIPLES FOR WORKING WITH PHYSICAL DOCUMENTS CONTAINING PERSONAL DATA:

- Work with them as if the documents contained your own personal data. Keep documents stored in a place that can be locked.
- When you are finished working with documents, please "lock them up" again.
- If possible, anonymise documents (for example, by blacking out all or some parts containing personal data).
- Only copy them if you have a clear need, and ideally only in anonymised form.
- When copying or printing documents – always collect them from the printer – do not let them "lie around" the printer.
- Always think about to whom and for what purpose you are giving documents.
- Only store documents for the time absolutely required and shred them once that period expires. Throwing documents in a waste-paper bin is not the proper way to discard them – use a shredder.
- If you encounter documents containing personal data and the owner cannot be ascertained, shred the documents.
- If you need advice or just a simple consultation on how to approach this type of document, do not hesitate to contact the Authorised Person in your section – see the list on page 2.
- Please do not forget that your monitors, too, feature a number of sensitive details and that, as a
- rule, whenever you leave your computer, lock it by using the keys "WIN+L".

9 Rules on Data Protection

1. ONE-ON-ONE APPROACH

Personal data is becoming a valuable commodity in the contemporary world. Given the nature of our work, we get masses of data about beneficiaries, course attendants, or social programme clients. That means that we are working with valuable "goods" that must be handled with great care, as we would handle our own personal data.

2. LAWFULNESS, ACCURACY, TRANSPARENCY

Personal data is any data on the basis of which a specific individual can be identified – from electronic data, such as an a-mail address, IP address, or cookies, to the most common data such as name and address, to sensitive

data such as information about one's health status or ethnicity. Personal data may also include photographs and audio/video recordings.

If you collect personal data, the person concerned must always be informed of it, including about the purpose for which you collect the data, how long you will hold it, and what will be done with it. In some cases, we must obtain, from the person concerned, an informed consent to the processing of his or her personal data.

3. PURPOSE AND RESTRICTION

You can only collect personal data if you have a reason: performance of an agreement, compliance with a legal obligation, legitimate interest, or informed consent. Personal data cannot be processed for any purpose other than that announced in advance – e.g., a journalist's contact details that we obtained in order to in inform him about our work cannot be used for the purpose of requesting a donation.

4. DATA MINIMISATION

Collect and use only the minimum amount of data you need for achieving your purpose. The regulation mandates us to collect and process only the minimum amount of data. All means and forms, scope of processing, and duration of storage must be appropriate to the purpose of processing. For example, if you are drawing up an overview for a donor, concerning the beneficiaries receiving food assistance, you will most likely not need to note the religious or ethnic affiliation; or, when collecting data about persons who have attended our workshops there is no reason to collect their ID numbers.

5. ACCURACY

Make sure that your data is up to date. When working with personal data, you should take measures to guarantee that inaccurate or erroneous data is not processed. Inaccurate data is not restricted to typographical errors; it includes formally incorrect data in relation to incorrect information.

6. LIMITED STORAGE

Do not store data longer than necessary. Personal data may only be processed for the minimum period required for the purpose concerned, and the data subject must be informed about the duration of the period (it cannot be an unlimited period of time). Upon the expiration of that period, data must be destroyed. A specific case of destruction is anonymisation of data – i.e., the destruction (deletion) of a part of data such that the specific individual cannot be in any way identified on the basis thereof.

7. INTEGRITY AND CONFIDENTIALITY

Keep data safe, password-protect it.Personal computer disks should not contain any personal data. Personal data should always be stored in places that are encrypted – i.e., on our servers, in section Share Points or personal One Drives.

Personal data on paper should always be stored in a lockable cabinet or in an office that is regularly locked. It is not good practice to have files containing personal data freely accessible, including during lunch break.

8. TRANSFER OF PERSONAL DATA

Do not pass personal data on to people who should not have access to it, not even within IDD.E-mail does not provide many security guarantees and hence it must be used with increased caution, and ideally no personal data should be sent by e-mail. If it is necessary to pass such information on, we recommend saving it in your section's Share Point or your personal One Drive disk and sharing it using the "Share" function. Another option is a password-protected archive (zip, rar), with the password being sent to the recipient via messaging application with "end to end" encryption (Viber or Messenger).

9. ACCOUNTABILITY AND CONTROL

We need to document how you process personal data. Our obligation imposed on us by the regulation is to make a record of processing activities. Hence, the Authorised Person of your section must be informed in advance about the processing of personal data in our own programmes (you can get that person's contact information from your operations manager, logistics department, or head of your section) and you need to consult the Authorised Person regarding any further steps to be taken, in order that we may always document that we process personal data in line with the regulation.