Data Protection Policy

Contents

Data Protection Policy 1
1 Purpose 2
2 Definitions 2
2.1 Data subject 2
2.2 Personal data 2
2.3 Sensitive data 3
2.4 Processing of personal data 3
2.5 Data controller and processor 3
3 Processing of persons data and sensitive data 3
4 Principles of data processing 3
5 Criteria of legitimate data processing 4
5.1 Providing information to data subjects 4
5.2 Obtaining consent 4
5.3 Registration 5
5.4 Ensuring the security of personal data 5
5.5 Respecting the rights of the data subjects 6
6 The data subjects' rights 6
6.1 Right to access information 6
6.2 Right to request rectification and deletion 7
6.3 Right to object to the processing 7
7 Requirements of data protection and security of data processing 8
8 Transfer of personal data to third countries 9
9 Data mapping 9
9.1 Clients' personal data 9
9.2 Data collected during monitoring 10
9.3 Partners' personal data 10

9.4 Staff members' personal data 10
9.5 Donors' personal data 11
10 Data Protection Officer 11
11 Data Protection Training 11
12 Data breach 11
13 Data Protection Officer 12

1 Purpose

Being an international human rights organisation that advances the rights of people with mental health issues or intellectual disabilities, Validity comes into contact with people – such as clients, donors, partners, people interested in receiving information – during its operation. In order to achieve its mission and operate its programmes, Validity needs to collect and use certain types of personal information related to the above individuals. Validity is committed to the protection of the personal data of its staff as well as that of its service users, partners and donors and is dedicated to ensure that personal information is collected, stored, recorded and processed appropriately.

The aim of this Data Protection Policy is to determine Validity's approach to data protection and to ensure that personal data and personal rights of its staff, service users and donors are protected by every means, no unauthorised person has access to the data processed by Validity and that such data does not become public. Therefore, Validity abides by the data protection requirements set out in the EU's General Data Protection Regulation (EU Reg. 2016/679) ("GDPR").

This Data Protection Policy was adopted on 25 May 2018.

2 Definitions

2.1 Data subject

Data subject is a natural person who has been identified by reference to specific personal data, or who can be identified, directly or indirectly.

2.2 Personal data

Personal data is any information that relate to the data subject, in particular by reference to their name, an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity and any conclusion drawn from such information in relation to the data subject.

2.3 Sensitive data

Sensitive data is personal data in relation to racial origin, national and ethnic minority origin, political opinion and party affiliation, religious or other ideological belief, membership of an interest group, sexual life, personal data in relation to health, pathological addiction and criminal personal data.

2.4 Processing of personal data

Processing of personal data is any operation or set of operations conducted upon personal data whether or not by automatic means. Operations include in particular collection, recording, organization, storage, adaptation or alteration, use, retrieval, transfer, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, and blocking from further use, photographing, sound and video recording and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples and retinal images).

2.5 Data controller and processor

Data controller is an organisation which collects data from EU residents. Data processor is an organisation that processes data on behalf of a data controller. Validity is a data controller within the meaning of the GDPR. Validity does not process data on behalf of other organisations.

3 Processing of persons data and sensitive data

In accordance with GDPR, Validity may process personal data if one of the following conditions are met (GDPR Article 6):

1. The data subject has given consent to the processing of personal data for one or more specific purposes.
2. Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.
3. Processing is necessary for compliance with a legal obligation to which the controller is subject.
4. Processing is necessary to protect the vital interests of the data subject or of another natural person.
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular if the data subject is a child.

4 Principles of data processing

Validity is committed to ensure that all principles of data processing listed below are adhered to.

- Personal data may only be processed for a specified purpose, to exercise a right or to perform an obligation. This purpose must be followed throughout all phases of data processing.

- Data processing must be fair and lawful.

- Only personal data that is indispensable and suitable to achieve the purpose of processing can be processed;

- Personal data can be processed only to the extent and for the duration necessary to achieve the purpose of data processing;

- Personal data must be accurate, complete and, if necessary, must be kept up to date;

- Identification of data subjects is possible for no longer than it is required for the purpose for which the personal data is processed.

5 Criteria of legitimate data processing

5.1 Providing information to data subjects

Before any data processing operation is carried out, Validity will inform the data subject whether their consent is required thereto or the processing is mandatory. Validity will also provide unambiguous and detailed information on request to data subjects on all relevant facts such as the sources from where the information was obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities relating to data processing, and if the personal data of the data subject is made available to others, the legal basis and the recipients.

5.2 Obtaining consent

Validity only processes personal data if the data subject has given their consent thereto, subject to the exceptions set out in section 3 above. Such consent must be voluntary, informed and individual and must be obtained in advance of data processing. In addition, if the data is transferred outside the European Economic Area (the "EEA"), the consent must be explicit, while in the case of processing sensitive data, a written consent is required, subject to the exceptions set out in section 3 above.

However, there may be cases, where data subjects are unable to give their consent e.g. if the data subject is a minor or is legally incapacitated. In such cases, the consent shall be obtained from the personal representative of the data subject, e.g. from his/her parents or guardian. If such representative gives the consent, Validity can process the data as if the data subject had given the consent.

If Validity cannot obtain consent from the data subject or from the representative and if there are no other legal grounds on the basis of whish Validity could process personal data, Validity may not process such personal data. If Validity collects or otherwise obtains any personal data for which Validity has not obtained the data subject's or their representative's consent, and if Validity wishes to continue to process any relevant information, Validity shall anonymise such information in a way that no personal data can be restored. As an example, faces of patients that appear on an image or video footage should be blurred in a way that such blurring cannot be removed, and the original image or footage must be deleted without the possibility of being restored. Likewise, a person's name, tax or social security ID and any other information, on the basis of which a specific person can be identified must be redacted from documents, and copies of the document that set out such personal data must be destroyed.

On the basis of the GDPR, data will not be considered personal data if it is anonymised in a way that the personal nature of the data cannot be restored by the controller of the data. The data subject is considered as identifiable as long as the data controller is in possession of the technical means which are necessary for identification.

5.3 Registration

Subject to certain exceptions, Validity is required to register data processing activities with the National Authority of Data Protection and Freedom of Information (in Hungarian: Nemzeti Adatvédelmi és Információszabadság Hatóság) (the "Authority") before the commencement of data processing within the territory of Hungary.

One of the exceptions from the registration obligation that could be relevant to Validity is where Validity processes personal data of private individuals who are in a contractual relationship with Validity, i.e. who are Validity's clients.

According to the Authority's practice, such exception applies if (i) data is collected directly from the data subject; (ii) the purpose of the data processing is known to the data subject; (iii) the types of the data to be processed and the term of data processing is determined in advance; (iv) data is processed in accordance with the predetermined purpose; (v) data is not processed by a third party controller; and (vi) data subjects received proper information.

This exception does not apply if personal data is processed for a purpose different from the purpose of the contractual relationship between the parties.

Validity has registered the following data processing activities:

- Registration decision no. NAIH-112710/2017: "Other. Validity collects data in order to carry out its charitable objectives, in line with the principle of informed consent. The purposes include public relations, engagement with mainstream and social media".

- Registration decision no. NAIH-112709/2017: "Other. Validity collects data in order to carry out its charitable objectives, in line with the principle of informed consent. The purposes include fundraising and donor relationship

5.4 Ensuring the security of personal data

Validity undertakes to take technical and organisational measures to ensure the security of personal data and undertakes to establish the procedural rules necessary for compliance with the legal regulations on data processing and other rules relating to data protection and confidentiality.

5.5 Respecting the rights of the data subjects

Data subjects have the following rights related to the processing of their personal data:

- Right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data (right of access)
- Right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her (right to rectification)
- Right to obtain from the controller the erasure of personal data concerning him or her without undue delay (right to be forgotten)
- Right to obtain from the controller restriction of processing (Article 18 GDPR)
- Right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller (right to data portability)
- Right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her
- Right not to be subject to a decision based solely on automated processing, including profiling

The above rights of the data subjects are described in more detail in Chapter 6 below.
Validity will handle any requests of the data subject in connection with the above rights in a timely and efficient manner in accordance with the applicable laws.

6 The data subjects' rights

6.1 Right to access information

Upon the data subject's request, Validity shall provide information concerning the data relating to them, including those processed by a data processor on its behalf, the sources from where they were obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities relating to data processing, and, if the personal data of the data subject is made available to others, the legal basis and the recipients.

In order to supervise the legitimacy of data transfers and for the information of the data subject, Validity maintains a transmission log, which records the time and date of

transmission, the legal basis of transmission and the recipient, description of the personal data transmitted, and other information prescribed by the relevant legislation on data processing.

Validity undertakes to satisfy the requests for information without any delay, and to provide the information requested in an intelligible form, in writing at the data subject's request, within not more than 30 days. With respect to any category of data, such information is provided by Validity free of charge once a year; however additional information concerning the same category of data within the same year may be subject to a charge. If any payment is made in connection with data that was processed unlawfully, or if the request led to rectification, such charge will be refunded by Validity.

6.2 Right to request rectification and deletion

If personal data is deemed inaccurate, and the correct personal data is at Validity's disposal, Validity undertakes to rectify the personal data in question.

Personal data shall be deleted by Validity (i) if processed unlawfully; (ii) if so requested by the data subject (iii) if the personal data is incomplete or inaccurate and it cannot be lawfully rectified, provided that deletion is not disallowed by statutory provision; (iv) if the purpose of processing no longer exists or the legal time limit for storage has expired; or (v) if so instructed by court order or by the Authority.

Personal data shall be blocked instead of deleted if so requested by the data subject, or if there are reasonable grounds to believe that deletion could affect the legitimate interests of the data subject. Blocked data shall be processed only for the purpose which prevented their deletion.

If the accuracy of an item of personal data is contested by the data subject and its accuracy or inaccuracy cannot be ascertained without doubt, Validity shall mark that personal data for the purpose of referencing.

If Validity refuses to comply with the data subject's request for rectification, blocking or deletion, the factual or legal reasons on the refusal shall be communicated in writing within 30 days of receipt of the request and Validity shall inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the Authority.

6.3 Right to object to the processing

The data subject shall have the right to object to the processing of data relating to them:

- if processing or disclosure is carried out solely for the purpose of fulfilling Validity's legal obligation or for enforcing the rights and legitimate interests of Validity, the recipient or a third party, unless processing is mandatory;

- if personal data is used or disclosed for the purposes of direct marketing, public opinion polling or scientific research; and

- in all other cases prescribed by law.

In the event of an objection, Validity shall investigate the cause of objection within 15 days, adopt a decision on the merits and shall notify the data subject of its decision in writing.

If Validity finds that the data subject's objection is justified, it shall terminate all processing operations (including data collection and transmission), block the data involved and notify all recipients to whom any of these data had previously been transferred concerning the objection and the ensuing measures, upon which these recipients shall also take measures regarding the enforcement of the objection.

If the data subject disagrees with the decision of Validity, or if Validity fails to meet the above 15 days' deadline, the data subject shall have the right to refer the matter to the court within 30 days of the date of delivery of the decision or from the last day of the time limit.

7 Requirements of data protection and security of data processing

Validity considers data protection and security of data processing as a priority. Therefore, Validity is committed to protecting data by means of suitable measures against unauthorised access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technology.

Validity ensures that for the protection of data sets stored in different electronic filing systems, suitable technical solutions are introduced to prevent the interconnection of data stored in these filing systems and the identification of the data subjects.

In the case of any automated personal data processing, additional measures will be implemented that are designed to:

- prevent the unauthorised input of data;
- prevent the use of automated data processing systems by unauthorised persons using data communication equipment;
- ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment;
- ensure that it is possible to verify and establish which personal data have been put into automated data processing systems and when and by whom the data were put in;
- ensure that installed systems may, in case of interruption, be restored; and
- ensure that faults emerging in automated data processing systems is reported.

8 Transfer of personal data to third countries

Personal data which is undergoing processing or is intended for processing after transmission may be transferred or disclosed by Validity to a data processor located in a third country only if the data subject has given their consent unambiguously to the proposed transfer/disclosure or if requirements of data processing set out in the GDPR are satisfied and the third country in question ensures an adequate level of protection. The protection shall be considered adequate if this fact is established by binding legislation of the EU or there is an international agreement between the third country and Hungary containing guarantees for the rights of data subjects regarding information, rectification and deletion, their rights to remedies and for the independent supervision and control of data processing operations.

In the interest of the implementation of an international agreement on international legal aid, exchange of information in tax matters and on double taxation, personal data may also be transferred to third countries in the absence of the above conditions, for the purpose and with the contents specified in such international agreement.

Transfer of data to EEA Member States is treated as if the transfer took place within the territory of Hungary.

Validity will ensure that contracts with its partners based in other countries include a clause on data protection, where those partners willingly undertake to be bound by rules under the GDPR and observe these in processing personal data.

9 Data mapping

Validity undertook an internal data audit to map the type of personal data collected by the organization. The following contain information about the purpose of collecting various data, and specific rules applicable to them.

9.1 Clients' personal data

Clients' personal data is collected for the purposes of representing them in legal proceedings. Their data is collected with their consent, which is part of the client engagement letter.

Clients' personal data is stored in electronic form on Validity's secured common drive (Sharepoint). Only staff working on the specific case and their supervisors have access to folders containing respective clients' personal data. Contacted external lawyers have access to folders that are containing data of their clients.

Court submissions include clients' personal data as necessary for the purposes of the court proceedings. This might include sensitive personal data, such as the results of psychiatric assessments, if these are relevant for the case.

A paper copy of the court file is kept at Validity's main offices. Files containing sensitive personal data are kept in a locked cabinet.

Case files are kept during the duration of the court proceedings, during the implementation proceedings, and for 7 years after the conclusion of the implementation proceedings for audit purposes. After the 7 year period passes, paper files are destroyed. Electronic copes of court correspondence are kept indefinitely.

Clients are individually asked for their consent to appear in media and our publications. They consent can be partial, they can specifically decide on the publication of their case information in an anonymized way, their name, their picture, statements, and video. Only personal data of clients who have given consent are used in publications. With other clients, Validity only uses information which is in the public domain, mainly which is part of court decisions.

Potential client's personal data is collected with their consent. If they become actual clients, the above rules apply. If the case does not progress to the courts, the case file is destroyed within a year of the final decision not to submit a court case.

9.2 Data collected during monitoring

Validity conducts monitoring of closed institution to document human rights violations. Monitoring results can be published as a report, or they can be used as evidence in court proceedings. Monitoring is an important way of fulfilling Validity's mission, protecting human rights of residents of institutions, which is a task carried out in the public interest.

During monitoring, Validity collects personal data about residents of institutions with their explicit consent. This includes their name, potential human rights violations they suffered, and their image. Images are only published in with the residents' face blurred, so that they are not identifiable. An unblurred image is kept as an electronic file only in the case of residents whom Validity might represent in a potential lawsuit and where the image might be used as evidence in the proceedings.

9.3 Partners' personal data

Validity works with a number of partner organizations, consultants and individual lawyers. It collects their personal data with their consent for the purpose of establishing a contractual relationship with them. Their personal data is accessible for staff members involved in project management involving the specific partners or lawyers. This includes the Legal Director, Campaign Director, and Finance Officer.

Contracts with partners, consultants and lawyers are kept on file as a hard copy for audit purposes for 7 years after the contractual relationship ends. Contracts are kept in electronic form indefinitely.

Validity reports to donors about its relationship with partners, consultants and lawyers, and produces to donors contracts, invoices and other documentation from partners.

9.4 Staff members' personal data

Validity collects their staff members' personal data for Human Resources management purposes (employment contracts, annual leave calculation, etc.). Hard copies of these files are kept in a locked cabinet, and are only accessible by the Finance Officer and the Administrative Assistant.

9.5 Donors' personal data

Validity collects the personal data of persons donating funds to our organization. We only collect data which these persons voluntarily disclose to us in their donation letters or statements.

10 Data Protection Officer

Validity's Executive Director was designed as a Data Protection Officer (DPO) in the meaning of the GDPR. The duties of the Data Protection Officer involve supervising Validity's compliance with the GDPR and this Data Protection Policy; organizing yearly training sessions for Validity staff on data protection requirements and obligations; and reporting data breaches to the authorities.

11 Data Protection Training

The Data Protection Officer will hold a training for Validity's employees on data protection requirements and obligations. The training sessions will be take place at least once per year for existing staff, and within a month of joining the organization for new staff members.

12 Data breach

If the case of a data breach, where unauthorized persons might have gained access to personal data processed by Validity either in physical or electronic form, Validity will notify the National Authority of Data Protection and Freedom of Information (in Hungarian: Nemzeti Adatvédelmi és Információszabadság Hatóság) (the "Authority") without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The notification referred to in paragraph 1 shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
e) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

Validity will document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Authority to verify compliance with the GDPR.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, Validity shall communicate the personal data breach in plain language to the data subject without undue delay.

13 Data Protection Officer

Validity will ensure that contracts with its partners based in other countries include a clause on data protection, where those partners willingly undertake to be bound by rules under the GDPR and observe these in processing personal data.