Privacy Policy

The Women For Women Together Against Violence Association (tax number: 18060339-1-42; email: info@nane.hu; hereinafter: NANE, or Association, or Data Controller,) as the data controller recognises the contents of the following legal statement as binding.

This Privacy Policy states NANE's guiding principles of data protection and management, as well as the Association's data protection and data management policy and procedure. It provides information to the Association's clients, contractual partners, those who visit the Association's website, and any other user about how their personal data is managed. The primary goal is for it to inform those involved in data management based on voluntary consent about their rights and options.

NANE commits to complying with all the requirements set by the present information brochure as well as the legislation in force regarding all data management related to their activities.

NANE is dedicated to protecting the personal data of their clients and partners and fnds it especially important to respect their clients' right to information-related self-determination. As a data controller and data processor, NANE manages personal data with privacy and implements all safety, technical, and operational measures that guarantee data security.

You, Dear Reader, provided the Association manages or processes some of your personal data, are entitled as a User to exercise your rights outlined by laws, with special regards to the right to adequate information.

Terms used in connection with data management

- **"personal data"**: any kind of data related to an identifed or identifable natural person ("user"); a natural person is considered identifable if they can be identifed, directly or indirectly, especially through one or several aspects related to some form of identifcation, for instance, name, number, data connected to their geographical location, online identifcation, or the natural person's physical, physiological, genetic, mental, economic, cultural, or social identity;
- **"data management"**: any kind of action or series of actions carried out on personal data or data fles in an automated or non-automated manner, such as collecting, recording, organising, structuring, storing, alteration or modifcation, query, inspection, usage, disclosure, transmission, propagation, or making available in any other way, coordination or interconnection, restriction, deletion, or destruction;

- **"data controller"**: a natural or legal person, public authority, agency, or any other entity that identifes the goals and means of personal data management on their own or together with other parties; if the goals and means of data management are determined by EU or member state law, the data controller or the special requirements related to appointing the data controller may also be determined by EU or member state law;

- **"data processor"**: a natural or legal person, public authority, agency, or any other entity that processes personal data in the name of the data controller;
- **"user"**: any given natural person directly or indirectly identifed or identifable based on personal data;

- **"third party"**: a natural or legal person, public authority, agency, or any other entity that is not the same as the User, the data controller, the data processor, or anybody else who has permission directly from the data controller or data processor to manage personal data;
- **"restricting data management"**: marking stored personal data with the aim of restricting future management;
- **"consent from the User"**: the User makes their will known based on clear and adequate information, in a voluntary and unambiguous way, by which the User, through a statement or action that unambiguously signals confrmation, gives their consent for their personal data to be managed;

- **“personal data breach”**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that is transmitted, stored, or managed in any other way.

The scope of personal data; the purpose, legal basis, and duration of data management

Data management by NANE is based on voluntary consent, contractual or legal obligation, or in some cases, on the legitimate interest of the data controller.

When personal data related to the User is collected from the Users themselves, the Association provides them with the entirety of the following list of information the moment personal data is collected:

1. the identity of the Data Controller or their representative; their contact details;
2. the intended purpose of personal data management, as well as the legal basis of data management;
3. if the personal data is not collected from the User: the categories of personal data in question;
4. in some cases, the recipients of personal data, or the categories of the recipients if this applies. Apart

from this information, the User will be notifed about the following supplementary information:

1. the duration of storing personal information, or if that is not possible, the aspects of determining said duration;
2. the User’s right to request the Data Controller to grant them access to their personal data, to correct, delete, or restrict the management of them, and the right to protest the management of personal data of this nature, as well as the User’s right to data portability;
3. in the case of data management based on voluntary consent, the User has the right to withdraw consent at any time, which does not afect the legality of the data management that was carried out based on their consent prior to the withdrawal;
4. the right to submit a complaint addressed to the supervisory authority;
5. whether providing personal data is based on laws or contractual obligation, or whether it is a prerequisite of entering into a contract; whether the User is obligated to provide personal data, and what the possible consequences of failing to do so are.

The User has the right to receive feedback from the Data Controller about whether the management of their personal data is in progress, and if so, they have the right to access the personal data and the following information.

The User has the right to request the Data Controller to correct any inaccurate piece of personal data, without any undue delay. Taking into account the purpose of data management, the User has the right to request the correction of incomplete personal data - through a complementary declaration, among others.

The User has the right to request the deletion of any piece of their personal data, without any undue delay, and the Data Controller is obligated to delete said personal data without any undue delay, provided other conditions are met.

The User has the right to request the Data Controller to restrict the data management if any of the following applies:

1. the User contests the accuracy of the personal data, in which case the restriction applies for the duration that allows the Data Controller to check the accuracy of personal data;

2. the data management is unlawful, and the User opposes deleting the data, instead requesting the restriction of its usage;
3. the Data Controller no longer needs the personal data for data management, but the User requests it for presenting, validating, or protecting legal claims; or
4. the User protested against the data management, in which case the restrictions apply for the duration it takes to determine whether the legitimate reasons of the Data Controller have a higher priority than those of the User.

The Data Controller informs any party that had access to the personal data about any corrections, deletion, or restricting of data, except if that is impossible or requires a disproportionate amount of efort. The User may request the Data Controller to inform them about said parties.

The User has the right to receive the personal data they provided to a data controller in a clear, widely used format that can be processed by computer, and they further have the right to send this data to another data controller without the data controller that has the personal data setting any obstacles, provided the data management is based on voluntary consent or a contract and happens in an automated way.

The User is entitled to be exempt from the efects of decisions that are based exclusively on automated data management - also including creating profles -, which would have legal efects or any similarly signifcant efects on them.

If a potential personal data breach occurs within NANE's system, which is likely to result in a high risk of adversely afecting natural persons' rights and freedoms, the Data Controller must also inform those individuals without any undue delay.

Storing personal data and the security of data management

The Association takes any necessary technical and operational measures in order to ensure the security of the personal data managed for any purpose or legal basis, as well as creates those rules of procedure that are necessary for enforcing the Regulation and the law about information-related self-determination and freedom of information.

The Association as data controller protects against accidental or unlawful destruction, loss, alteration, damage, unauthorised disclosure of, or access to data in its possession with the appropriate measures. It expects the same level of diligence from the agents and contractors in charge of data processing, fxing their obligations in a contract.

NANE's computer systems and other places of data retention can be found in its headquarters as well as on the relevant servers.

NANE chooses and operates the IT devices used for personal data management during its services based on the following criteria:

- it can only be accessed by those that have authorisation;
- its authenticity and authentication are ensured;
- its constancy can be verifed;
- it is protected against unauthorised access.

Access to personal data in relation to the specifc activities of the Association will be further expanded upon under Services.

The Association protects the IT systems used to process personal data with frewalls and virus protection services.

The parts of the Association's IT system, the confgurations, the manufacturers of the IT devices, the names of licensed software, the safety settings, and the types of frewall all constitute a trade secret and are considered to be confdential information, thus, they cannot be fully listed in the present Policy.

NANE protects data with the necessary measures, especially against unauthorised access to, alteration, transmission, disclosure of, deletion, or destruction, as well as against accidental destruction, damage, and inaccessibility caused by changes in the relevant technology. Taking into consideration the current levels of technology, it ensures the protection of the security of data management with appropriate technical, operational, and organisational measures, which can provide adequate protection against the risks connected to data management.

Nevertheless, we inform the Users that electronic messages transmitted through the internet, irrespective of protocol (e-mail, web, FTP, etc.), are subject to network threats that lead to fraudulent activities, the contesting of the contract, or the disclosure and modifcation of data. NANE vows to take any reasonable precautionary measures to protect from such threats.

The Association ensures the monitoring of electronic incoming and outgoing communication in order to protect personal data.

In a working context, only the respective administrators can access the documents under processing. The documents in paper format and their copies - provided they include personal data - are stored in a safe way in the Association's headquarters.

The Association ensures the appropriate physical protection of data, as well as the documents and devices holding said data. For this purpose, a data protection and data security policy was implemented, the compliance with which is also expected of the Association's volunteers and employees.

Respective volunteers, as well as internal employees, are the ones primarily authorised to access data managed by NANE. Data is not transmitted to third parties unless there is a legitimate interest (e.g. debt collection), legal obligation, or if the User has previously given their explicit consent.

Besides physical and IT security, it is especially important to develop and maintain awareness. Therefore, the Association makes sure to inform volunteers and employees, ensures that rules are respected, and organises training related to data protection at specifc intervals to refresh knowledge.

Data management based on individual rights*

(*data management is determined by the Association, with authorisation based on laws or given by Users)

Phone-based data collection for the helpline

During the conversations that take place through the helpline, the Association collects data provided by the caller in a short written summary in order to ofer help and provide information. The legal basis of this type of data management is *consent from the User,* expressed via implication and by continuing the conversation after having been verbally informed about it.

The caller is thus informed about the data recording when their call is received. If the User consents to the data recording, the conversation continues, and the caller is entitled to the rights of the User previously listed. The caller may ask for their data not to be recorded. In this case, no note is made of the call.

The Association keeps the following data about phone call records:

1. the caller may provide any information during the call that is recorded in a written summary;
2. if publications are sent by post: name and address must be provided;
3. the legal position of the caller (information about their court cases, their children, their own health conditions and those of their relatives, etc.);
4. the time and duration of the call.

A voice recording is never made of the calls.

Duration of the storage: 10 years (the recorded data can be traced back based on the phone number and/or the exact date and time of the call).

Persons authorised to access the data: the Association's volunteers, those in training to be volunteers, and their substitutes, as well as members of the Association responsible for tasks related to customer service.

Data transmission: does not happen automatically, only on the request of an authorised person, or on an ofcial request when fulflling legal obligations. Courts, the prosecutor's ofce, investigating authorities, infringement authorities, administrative authorities, the Hungarian National Authority for Data Protection and Freedom of Information, and other authorities based on statutory authorisation may ask the Data Controller to provide information, transmit data, or grant access to the documents. Based on the inquiry from such authorities, in addition to the designation of the exact purpose and data by the inquirer, the Association provides the personal data that is indispensable for realising the other authority's purpose.

If in the future the Association transmits the personal data procured in a lawful manner to parties other than those listed in this Policy, it will inform and ask for the User's consent regarding this fact, its legal basis, the name of the addressee, and any other signifcant circumstance of the data management/processing, at the latest at the frst disclosure of personal data.

The Association transmits personal data to third countries or international organisations only on the explicit request of the User, with their written consent.

Cookies

When visiting the www.nane.hu website, the service provider sends one or multiple identifcation marks (cookies, to use the technical term) - meaning a small fle containing a series of characters - to the device of the User, as a result of which their browser will become individually identifable. These cookies will only be sent to the visitor's device when visiting certain subpages; therefore, only the fact that the subpage was visited and the time when it happened are stored; no other information is recorded.

The cookies thus sent are used in the following way: external service providers, including Google, store with the help of such cookies whether the User has visited the NANE website before.

If the User does not want Google or any other service provider to track their data in the way and for the purpose mentioned above, we advise installing a blocking extension to their browser.

In the menu bar of most browsers, there is a Help function which provides information about how you can

- block cookies,
- allow new cookies, or
- get your browser to set new cookies, or
- block other cookies in the browser.

Community directives / Data management on the Association's Facebook page

In order to inform about and promote the Association's operation and services, as well as to keep in contact, the Association maintains a Facebook page:

The personal data shared by visitors on the Association's Facebook page is not managed by the Association, nor can it take responsibility for this data considering that it is a service available for free and accessible by anyone.

Therefore, Facebook's own Data Policy and Terms of Service apply to visitors (https://www.facebook.com/privacy/explanation).

Questions and reports shared on the Association's Facebook page are not considered an ofcial complaint.

In the case of unlawful or ofensive posts, the Association may ban the User from among the members or delete their comment without any warning.

The Association is not responsible for the content or comments that violate the law published by Facebook users since it has no infuence on their publication. After becoming aware, the Association immediately removes such contents from the Facebook page - provided the technology allows it.

The Association is not responsible for any errors or malfunctions connected to Facebook's operation, or problems stemming from changes in the system's operation, e.g. data loss, data theft, etc.

The Association warns Users sharing personal data in the comments that it is a public platform, so they should act accordingly.

E-mail and Facebook letters seeking help

The Association handles messages sent to the info@nane.hu e-mail address, or in the form of answered by the Facebook private messages, in the following manner. Incoming letters are Association's employees and volunteers.

In order to ofer help, data provided through electronic communication with the Association will be recorded. The legal basis of this type of data management is *consent from the User,* expressed via implication when they contact the Association.

Facebook's Data Policy applies to storing the messages communicated on the platform. The letters sent by email (including those that arrive through the nokjoga.hu/kapcsolat and muszajmunkacsoport.hu/contact websites) are stored for 5 years.

Fundraising and Registration of Donations

Donation-related Data Management:
Administer information in a database considering incoming donations - including online bank card payments, 1% tax offers, postal checks, bank transfers, and direct debit orders - categorized by donors and campaigns.

Purpose of Data Management:
Complying with our reporting and registration obligations, expressing gratitude, and maintaining contact.

Legal Basis for Data Management:
GDPR Article 6(1)(a) and (c).

Scope of Managed Data:
Name, email address, telephone number (if provided), address (if provided), payment method, last 4 digits of bank card (if provided), bank card expiration date (if provided), and bank account number (if provided), unique identification code, donation amount, currency, date and regularity of donation(s), additional comments made by the donor, registration of the name or statistical number of the donation project, and the donor's connection with NANE.

Planned Deadline for Data Management:
Until the seventh year after the donation was made or until the tax statute of limitations expires.

Newsletter subscribers

Mailchimp's system is used; the Association's employees and external contractual partners in charge of sending the newsletter can access this list. Data is not transmitted to third parties. Names and e-mail addresses are managed with the consent of the User. You can unsubscribe from the newsletter at any time. In order to modify your data, contact the info@nane.hu e-mail address.

The rights of the User

The User has the right to request the Association as the data controller to grant them access to their personal data, to correct, delete, or restrict the management of said data, and to protest the management of such personal data by an e-mail or letter sent to the Association by post.

The User - under certain legislative conditions - has the right to receive the personal data they provided to a data controller in a clear, widely used format that can be processed by computer, and they further have the right to send this data to another data controller without the data controller that has the personal data

setting any obstacles. The User also has the right to ask for their personal data to be directly transmitted among data controllers - if the technology allows it.

In the case of data management based on voluntary consent, the User has the right to withdraw consent at any time, which does not afect the legality of data management that was carried out based on their consent prior to the withdrawal.

If the User disagrees with the data management (its legal basis, purpose, methods, etc.), they have the right to make a complaint to the supervisory authority (contacts at the end of the document).

Incident management

Personal data breach: means the violation of the personal data's integrity and confdentiality; a violation of security that leads to the accidental or unlawful destruction, loss, modifcation, unauthorised disclosure of or access to the personal data transmitted, stored, or managed in any other way.

Personal data breaches are a threat to the Association both as a data controller and a data processor. However, risks can be minimised through adequate preliminary actions and developing quick response methods.

We ask our Users to inform us immediately if they notice personal data breaches or anything indicating personal data breaches in how their own or others' personal data is managed within the Association's operation. The forums of reporting personal data breaches are:

- **the main email address of the Association: info@nane.hu;**
- the postal address of the Association: 1447 Budapest P.O. Box 502.

In the case of a personal data breach, the president (decision-maker) of the Association identifes and isolates the systems, persons, and data in question, then they make sure to collect and store the evidence as proof of the personal data breach. They then start to repair the damages caused and restore the lawful operation.

The Association keeps a record of personal data breaches.

Customer relationship

Should you have any remarks, questions, or problems with our Association, data management policy, or our services, you can withdraw your previous consent and ask for the deletion or modifcation of your data through the following channels:

- by e-mail at info@nane.hu, as well as
- by post addressed to 1447 Budapest P.O. Box 502.

Miscellaneous

We inform about data management not listed in this Policy when the data is recorded and the legal basis of the data management is created. E.g. data management of our contractual partners and contact persons.

The Association reserves the right to unilaterally modify this data management policy after informing the Users.

The Association does not verify the personal data it receives. The validity of the data is the sole responsibility of the person providing it. When giving their email address, the User takes responsibility for being the sole person using said e-mail address to access services.

Rules of procedure

The Data Controller has 30 days to inform about, delete, and correct personal data. If the Data Controller does not fulfl the User's such requests, they will state the reasons for refusal in writing within 30 days.

Data Protection Authority

You may turn to the Hungarian National Authority for Data Protection and Freedom of Information with any complaints:

Hungarian National Authority for Data Protection and Freedom of Information, 22/C Szilágyi Erzsébet fasor, Budapest, 1125, Mailing address: 1530 Budapest P.O. Box 5, Phone number: 06.1.391.1400, Fax: 06.1.391.1410, E-mail: ugyfelszolgalat@naih.hu, Website: http://www.naih.hu