

PRIVACY POLICY

1. Data controller

Who can you turn to if you have a question?

Name: Greenpeace Hungary Association

Address: 1143 Budapest, Zászlós u. 54.

Representative of the controller: János Bálint Mező

Data Protection Officer of the controller: Balázs Dobos

Contact of the Data Protection Officer: privacy.hu@greenpeace.org

Present guide is the unilateral commitment of the Data Controller, in accordance with Regulation (EU) No 2016/679 of the European Parliament and of the Council (27th April 2016) [hereinafter: GDPR] and the approximating laws of the Member States.

Present Regulations may be unilaterally modified and/or cancelled by the Data Controller, who shall simultaneously inform the Subjects. Information provision may be attained either by the publication of information on the website or by direct communication to the Subjects, depending on the nature of the modification.

2. Purpose of Data Processing

What kind of data we ask for and how do we use it?

2.1 Fundraising and registering donations

Processing incoming donations in a database, (especially: direct debit, online credit card payment, 1% tax donation, postal cheque and money transfer) by donor and campaign.

Legal basis of data processing: Performance of contract

Scope of processed data:

- Name
- Email address
- Last four digits of credit card number (if provided)
- Expiry date of credit card (if provided)
- Bank account number (if provided)
- Unique identifier
- Amount donated
- Date(s) of donation
- Registration of the name or statistical number of the fundraising project

Envisaged deadline of data processing: 8 years

2.2 Donor registration

Retaining and registering proof of payment, in compliance with accounting obligations.

Legal basis of data processing: Legal obligation

Scope of processed data:

- Name
- Email address
- Last four digits of credit card number (if provided)
- Bank account number (if provided)
- Unique identifier
- Amount donated
- Date(s) of donation
- Registration of the name or statistical number of the fundraising project

Envisaged deadline of data processing: 8 years

2.3 Petition campaigns

Registration of those joining petition campaigns, proof and documentation of joining.

Legal basis of data processing: Consent of data Subject

Scope of processed data:

- Name
- Email address
- Phone number
- The fact of having signed the petition and the date
- Name of petition
- Log file

Envisaged deadline of data processing: until revocation

2.4 Processing data of persons targeted with a project

Storage of contact data of persons targeted with a petition or project.

Legal basis of data processing: Legitimate interest - It is imperative for the core business of the organisation to process the data of those to be addressed in relation to projects and petitions.

Source of processed data: public data, websites, data published in official notices

Scope of processed data:

- Name
- Job title
- Phone number
- Postal address
- Email address

Envisaged deadline of data processing: Opposition of Subjects concerned

2.5 Communication, eDM, DM, telephone

Sending messages about campaigns of the organisation, about opportunities for engagement; getting in touch with subscribers, supporters and former supporters by email and on the phone; sending postal cheques and promotional material by post, sending birthday messages.

Legal basis of data processing: Consent of data Subject

Scope of processed data:

- Email address

- Postal address
- Name
- Phone number
- Log file
- Date of birth

Envisaged deadline of data processing: until revocation

2.5.1 Segmented communication, eDM, DM, telephone

Based on the specific consent of the persons concerned, segmented communication about topics that command the person's interest / were chosen by the person in question.

Legal basis of data processing: Consent of data Subject

Scope of processed data:

- Email address
- Postal address
- Name
- Phone number
- Log file
- Date of birth

Envisaged deadline of data processing: until revocation

2.6 Press communications

Press releases in electronic form, invitations for press events, press communications on the homepage of Data Controller.

Legal basis of data processing: Consent of data Subject

Source of processed data: Consent of data Subject

Legal basis of data processing: Legitimate interest

Source of processed data: data from public sources

Scope of processed data:

- Email address
- Name
- Phone number
- Name of media
- Log file

Envisaged deadline of data processing: until revocation or, in case of legitimate interest, until opposition

2.7 Documenting events, information to the public

Publishing photos and videos made during events on public media outlets of the Data controller and in the press.

2.7.1 Preparation and publication of mass imagery for the purpose of documenting the event, informing the public, presenting and promoting the activities of the Data Controller.

Mass imagery is a photo or video recording that captures the events as a whole, such as recordings made at an event or its individual programs or classes, in which several participants are visible.

Scope of processed data: image of the participants in the programs on a mass recording.

Legal basis for data processing: legitimate interest.

Deadline for data processing: until there is a legitimate interest.

2.7.2 Preparation and publication of individual recordings for the purpose of documenting the event, informing the public, presenting and promoting the activities of the Data Controller.

This includes photo or video recordings that explicitly and identifiably shows a particular participant in the event, such as a portrait of a person, and so on.

Scope of processed data: a unique image of the participants in the programs.

Legal basis of data processing: The consent of the Data Subject, which in the case of announced public mass events, is expressed in action, ie by participating in the public event. In other cases, the Data Subject shall give consent in an electronic or written statement.

Envisaged deadline of data processing: until revocation.

2.8 Recruitment of volunteers, communication and travel arrangements

Registration of volunteers who have signed up on the web. Invitation for the Info Day, filling out the attendance list on the Info Day. Communication aimed at volunteers about opportunities for engagement and events. Travel arrangements for volunteers visiting events or trainings and travel insurances relating to these.

Legal basis of data processing: Consent of data Subject

Scope of processed data:

- Name
- Postal address
- Date of birth
- Email address
- Phone number
- Log file
- ID number
- Passport number

Envisaged deadline of data processing: until revocation

2.9 Recording the data of members of the association and recording natural persons present at the general meeting

Convening general meetings, sending invitations, registering, processing and storing the data of the participants

Legal basis of data processing: Legal obligation

Scope of processed data:

- Name
- Address
- Signature

Envisaged deadline of data processing: In accordance with the provisions of the law, 8 years after the termination of the operation of the association.

2.10 Organisational administration, work organisation, improving labour efficiency

Processing and registration of incoming invoices, handing them over to the account department, contacts with partners

Legal basis of data processing: Legitimate interest - It is in the legitimate interest of the organisation to carry out data processing in the interest of improving the efficiency of work organisation

Scope of processed data:

- Name
- Postal address

Envisaged deadline of data processing: 8 years

2.11 Operation of an electronic video monitoring system in protection of the following:

- To protect the safety of the establishment of the Data Controller
- To protect the capital goods of the Data Controller
- To protect the physical security and the capital goods of the employees and visitors of the Data Controller
- To investigate the circumstances of any criminal offences or accidents that may occur

Legal basis of data processing: Consent of data Subject which, in this case, consists in the act of entering the establishment of the Data Controller, in spite of the warning about the video monitoring system.

The above mentioned activities are carried out by the Data Controller in accordance with Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators (Security Services Act).

Scope of processed data:

- Picture and moving image of natural persons (hereinafter recordings)

Envisaged deadline of data processing: 3 days

2.12 Data processing in relation to GDPR

Data processing, data transfer register, data protection incidents, needs and queries of those concerned

Legal basis of data processing: Legal obligation

Scope of processed data:

- Name
- Data protection identification number
- Claim of Subject, date, type, content
- Outcome of claim of Subject
- Date, documentation and outcome of incident

Envisaged deadline of data processing: Not to be discarded

2.13 Contacts with representatives of contractual partners:

- Identification of representative, distinguishing representative from other representatives
- Contacts, Processing and recording the data of correspondents
- Processing documents related to personal contacts and visits to partners
- Update and reconciliation of correspondent data
- Participation at events and ancillary services related to these

Legal basis of data processing: Legitimate interest - It is in the legitimate interest of the Data Controller to process the data of the correspondents of its business partners, pursuant to the fulfilment of the contract.

Scope of processed data:

- Name
- Postal address
- Email address
- Phone number
- Unique identifier

Envisaged deadline of data processing: On the last workday of March, 4 years after the termination of the contract

2.14 System messages

Sending system messages to Subjects, especially under the following circumstances:

- Receipt, failure, cessation, renewal of donation;
- Confirmation of having signed petition;
- Reconciliation and clarification of data;
- Data procession incident

Legal basis of data processing: Legitimate interest

Scope of processed data:

- Email address
- Name
- Phone number

Envisaged deadline of data processing: Until opposition / termination of contract between Data Controller and Subject

2.15 Advertising service(s), information provision for Subjects

Notice of new or renewed services, advertising, direct marketing or marketing communication, invitation for marketing events and conferences.

Being a non-profit organisation, the amount raised by our "marketing" activities is used in pursuance of our public benefit purposes.

Legal basis of data processing: Legitimate interest - Direct marketing is in the legitimate interest of the Data Controller

Scope of processed data:

- Email address
- Phone number
- Name
- Postal address

Having previously used certain services, Subject has provided Data Controller with their data. Data Controller informs the Subject, by way of this guide, that on the grounds of legitimate interest, it reclassifies the purpose of data processing with regards to the data processed in relation to the activities specified above under point 2 and uses the data in question for the purposes of direct marketing.

Source of data: Data Controller legitimately processed the data of the Subjects for a different purpose.

Envisaged deadline of data processing: Until opposition

2.16 Organisation of events and programmes subject to registration

Record of registered participants of professional programmes, conferences, trainings and communication in relation to the event with the participants.

Legal basis of data processing: Consent of Subject

Scope of processed data:

- Name

- Email address
- Phone number
- Postal address
- Information concerning the participation at the event (programme preferences, meals, etc.)

Envisaged deadline of data processing: until the end of the 3rd month following the end of the event and related communication.

2.17 Professional cooperation, community campaigns

Furthering the aims of the organisation with external partners and community effort. Communication and contacts with partners.

Legal basis of data processing: Consent of Subject

Scope of processed data:

- Name
- Email address
- Phone number
- Postal address

Envisaged deadline of data processing: until revocation

2.18 Measuring client satisfaction, survey of the opinion of followers and supporters

Questionnaire-based survey amongst followers and supporters of the organisation, collection of feedback on environmental protection and on the work of the organisation, channelling feedback into the work of the organisation.

Legal basis of data processing: Consent of Subject

Scope of processed data:

- Email address
- Gender
- Age
- Answers given on questionnaire (which do not qualify as personal data)

Envisaged deadline of data processing: until revocation

3. Scope of Subjects

Whose data do we process?

Natural persons who promote the activities of the organisation or take part in these, who follow or support the organisation, who enter the premises of the organisation, who are members of the association and who wish to be present at the public general meeting of the organisation.

4. Scope of compulsory data

On data provision platforms where all fields are compulsory to be filled in, Data Controller does not specifically indicate compulsory data. On those platforms where not all fields are compulsory, Data Controller indicates the compulsory fields by asterisks*.

5. Consequences of failure to provide data

Potential consequence of failure to provide data: failure to achieve the purpose of data processing.

6. Children

Persons under the age of 16 may not provide personal information about themselves unless they have the permission of their parents or legal representative.

By providing the information, the Data Subject declares and warrants that he / she will act in accordance with the above, and that his / her capacity to act in connection with the provision of the information is not limited. If the Data Subject is not legally entitled to provide the information independently, he / she is obliged to obtain the consent of the relevant third parties (eg legal representative, guardian). In this context, the Data Subject is obliged to consider whether the consent of a third party is required in connection with the provision of the given information. It may happen that the Data Controller does not come into personal contact with the Data Subject and does not become aware of his or her age, so in this case the Data Subject is obliged to ensure compliance with this clause, and the Data Controller is not liable in this connection.

If the Data Controller becomes aware that they have been in contact with a person under the age of 16, they shall make a reasonable effort to verify the existence of parental custody consent. Or, if personal data subject to consent has been obtained from a person under the age of 16 without the consent of the legal representative, the Data Controller shall take the necessary steps to delete the data as soon as possible.

7. Information about the employment of data processors

In the course of data processing, Data Controller transfers the data to contracted data processor(s) for performance of the contract.

Categories of addressees: postal and courier services, shipping companies, IT operators, web hosting service providers, web content developers, accounting service providers, security service providers, Internet payment service providers, travel agencies, airlines, insurance companies, accommodation providers, eDM providers, CRM providers, telemarketing companies, legal advisors, GDPR advisors, business advisors, social media sites, web-based application providers.

7.1 Data transfers to non-EEA countries and safeguards

The Data Controller transfers the data of users to the following addressees, as data processors:

Non-EEA addressee	Safeguards of data transfer
Google	Standard Contractual Clauses (SCC)
Engaging Networks	With adequacy decision
Facebook	Standard Contractual Clauses (SCC)

Greenpeace International and its national and regional offices	Transfer agreement based on Commission Decision 2004/915/EK
--	---

8. Those entitled to be apprised of the data

With the exception of the data processor(s) listed under point 7, Data Controller will not transfer the data accessed to any other parties. The data recorded can only be accessed by the employees of the Data Controller and by appointed employees of data processor(s).

8.1 Access to data recorded by the electronic video monitoring system

The Data Controller does not publish the recordings of the electronic monitoring system.

With the exception of the security service provider indicated in point 8 or law enforcement authorities, Data Controller will not distribute video recordings to any other parties. Recordings can only be accessed by the employees of the Data Controller and by appointed employees of data processor(s).

Recordings made by the electronic video monitoring system can only be accessed by the Data Protection Officer, the Head of Office, the IT Operator and the Executive Director. Upon request, Subjects can access the recordings made of themselves, in the presence of one of the persons mentioned above. Access always must be requested from the Data Protection Officer in writing.

Data Controller shall draw up a report about the access, which the organisation will keep for 1 year.

8.2 Limiting the deletion of the recordings made by the electronic monitoring system

Deleting the recordings after 3 days made by the electronic monitoring system can only be limited if the Data Controller experiences an event which is likely to jeopardize the purpose of the electronic monitoring system.

Upon request, deletion of the recordings can only be limited concerning recordings made of the Subjects themselves. Blocking must be requested from the Data Protection Officer in writing, indicating the purpose and the expected duration.

Data Controller shall draw up a report about every step in the blocking process. The report will be stored by the Data Controller for 1 year.

9. Automatic decision making

Data Controller maintains an automatic email notification system, the principles of operation of which are as follows:

9.1 Automatic birthday messages

Logic of functioning of the system: Every year, on the date of birth provided by Subject, Data Controller sends a birthday message to the email address provided.

Consequence of automatic decision making for the Subject: Pertaining to the processing of personal data, it has no direct consequence for the Subject.

9.2 Automatic greeting process

Logic of functioning of the system: When Subject is newly included in the database of the Data Controller and consents to the purpose of data processing as described in point 2.5, they receive a

round of unique, electronic mails at the email address provided, introducing them to the activities of the Data Controller and to opportunities of being involved in these. The content of the individual letters is chosen automatically by the system, based on whether the person concerned have read the previous email and whether they have used opportunities to get involved.

Consequence of automatic decision making for the Subject: Pertaining to the processing of personal data, it has no direct consequence for the Subject.

9.3 Segmented newsletter

Logic of functioning of the system: Subject indicates important options pertaining to the segmentation (for example on a petition site or questionnaire) and consents to receiving segmented communication material they might be interested in based on their answers, from the Data Controller. When sending individual emails, the mailing system of the Data Controller automatically selects the addressees belonging to a given segment (based on previous consent and answers).

Consequence of automatic decision making for the Subject: Pertaining to the processing of personal data, it has no direct consequence for the Subject.

10. Processing of data provided by third party

If a User/Partner does not provide their own data but that of another natural person, it is the sole responsibility of the User/Partner to make sure that the natural person in question has been adequately informed, is aware of and consents to the provision of the data. Data Controller is not required to determine whether this is the case. Data Controller calls the attention of the User/Partner to the fact that if – due to their not complying with the above mentioned obligation – Subject seeks legal recourse against Data Controller, Data Controller may delegate the claim and the amount of the damage to the User/Partner.

11. Rights of Subjects

Using the contacts specified in point 1, Subject may request the Data Controller to

- provide information about the processing of their personal data
- to correct their data
- to provide information on data processing
- to delete their personal data and to restrict data processing
- to transfer their data to another Data Controller, if the data processing is based either on a contract or on consent and the Organisation processes it through an automated procedure
- make provision for the withdrawal of their consent pertaining to the data processing

Subject may exercise the above mentioned rights at any time.

At the latest within a month following the submission of the request – or, in an exceptional case, within a longer deadline permitted by law – Data Controller shall fulfil or deny the request (explaining its reasons). Data Controller shall inform the Subject about the result of the inquiry.

11.1 Cost of information provision

The Organisation shall take relevant measures and provide the relevant information **free of charge** once a month.

If Subject requests the same, unchanged data for a second time within the same month, Data Controller will charge an administration fee.

- The cost of administration shall be calculated based on the hourly rates of the minimum wage.
- The number of work hours spent on the provision of the information, calculated at the hourly

rate mentioned above.

- In case of a paper-based information provision request, the cost price of printing and posting.

11.2 Refusal of information provision

If the request of the Subject is manifestly **unfounded** – they are either not entitled to the information or the Organisation as Data Controller can prove that the Subject is in possession of the requested information – the Data Controller shall refuse to provide the requested information.

If the request of the Subject is **excessive**, especially concerning its frequency, the Organisation may refuse to act on the claim if

- Subject requests to exercise their rights in relation to the same subject – with reference to Article 15-22 of the GDPR – for the third time within the same month.

11.3 Right to object

Subject is entitled to object to the procession of their personal data on the legal basis of legitimate interest or public authority, at any time.

If that is the case, the Organisation is obliged to stop the procession of the personal data, unless it demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data Subject, or relate to the presentation, assertion or protection of legal claims.

If the legal basis of the objection is justified, the Organisation shall stop the procession of the data – including the transfer of the data and recording any further data – as soon as possible. It shall also notify all transferees about the objection.

Compliance with the request is free of charge, unless the request is unfounded or excessive, in which case the Data Controller may charge a reasonable fee, proportionate to the cost of the administrative services provided. If the Subject does not agree with the decision made by the Data Controller, they may refer the matter to the court.

12. Data transfer to third countries or to international organisations

Except for point 7-8, the Data Controller transfers NEITHER the personal data of the Subject, NOR the recordings to any non-EEA or third country or to any international organisation.

13. Information on data security measures

Data is handled by the Data Controller in a closed system, as called for by the Information Security Regulations.

Data Controller ensures data protection by default and by design. For that purpose, Data Controller applies relevant technical and organisational measures in order to:

- precisely regulate access to the data;
- only allow access to persons who need the data in order to be able to carry out work with the data and even then, only to the amount of data minimally necessary to accomplish the task;
- choose appointed data processors carefully and ensure the security of the data by appropriate data processing contract;
- ensure that the processed data remains unaltered (data integrity), authentic and secure.

Data Controller employs reasonable physical, technical and organisational security measures in order to protect the data of subjects, especially to prevent incidental, unauthorised or unlawful distraction of the data, loosing, altering, transferring, using, accessing or processing of the data. Should Data Controller become aware that data was accessed or used in an unauthorised manner and this poses a high risk to the Subject, Data Controller shall inform the Subject without delay.

If a subject's data needs to be transferred, Data Controller adequately ensures the security of the data to be transferred, for example by encrypting it. Data Controller shall be liable for any data processing carried out by a third person on subject data.

Data Controller also ensures the protection of the data of the Subject against destruction or loss by adequate and regular backups.

14. Analytical services, cookies

Data Controller uses cookies and following codes of external service providers (especially Google and Facebook) in order to create website statistics and to measure user interest, demographic data and behaviour on the website. In addition to the above, Data Controller may use accumulated data gained from personalised advertising services or visitor data (for example age, gender and sphere of interest) in order to prepare and develop general website reports or in order to use the data for the purposes of advertisement marketing.

The aim of the above is to regularly develop our Internet platforms and to increase the efficiency of the advertisements relating to our campaigns.

On the [Ads Settings website](#), provided by Google, the Google Analytics service can be turned off for Display advertisements and the advertisements of the Google Display Network can be personalised.

Furthermore, all monitoring carried out by Google Analytics can be blocked with the help of the browser module [available here](#).

In order to display targeted advertising, we also use the remarketing code of Facebook. If you do not wish to see advertisements based on your site visits and interests, the service can be turned off using [this link](#).

You may find further information about the use of cookies on the website allaboutcookies.org – among others, there is a detailed guide about how to delete cookies from your computer. In order to find out how to delete cookies from your mobile phone, you need to consult the manual of your device.

By using the website, you consent to the use of technical data and cookies as described above. It is important to know that these, in themselves, cannot be used to identify a person and that after you leave the website, they become deleted in accordance with the settings of the browser.

15. Legislation applied

Provisions of the law relevant to the data processing carried out by the Data Controller:

- regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "GDPR"),
- act CXII of 2011 on informational self-determination and freedom of information (hereinafter "Info act")
- act C of 2000 on accounting (hereinafter "Accounting act"),
- act V of 2013 on the civil code (hereinafter "CC"),
- act CLV of 1997 on consumer protection (hereinafter "Consumer protection act")
- act CXXXIII of 2005 on Security Services and the Activities of Private Investigators (hereinafter "Security Services Act")
- Act CLXXV of 2011 on the Freedom of Association, Non-profit Status and the Operation and Support of Civil Organizations

16. Appeals

Should you have any questions or problems, please contact us so that we can settle the issue as soon as possible. If you are still not satisfied or feel that your rights have been prejudiced, you may turn to the institutions below.

Any Subject whose rights relating to the processing of their personal data have been presumably prejudiced may turn to the competent court, in the capital to the Capital Regional Court too, or may initiate an investigation at the National Authority for Data Protection and Freedom of Information.

President: dr. Péterfalvi Attila,

Address: 1055 Budapest, Falk Miksa utca 9-11.,

Contacts: ugyfelszolgalat@naih.hu, +36-1-3911400, www.naih.hu

Budapest, 5th October 2020