Privacy Policy – A Drop in the Ocean

Applicable as of June 07th, 2018
Updated January 16th 2023 / Version: 5

Content

1 Introduction

1.1. Purpose

A Drop in the Ocean's (Dråpen i Havet, hereafter DIH) intention with this Privacy Policy is to document the way we handle registered persons and users' data and that we process this in accordance with Norwegian privacy legislation as well as the EU's General Data Protection Regulation (GDPR). The policy provides an overview of the rights of registered persons data. It explains what personal data DIH collects, processes and stores and for what purpose. It also explains how to request insight to or deletion of the users' personal data. Further it explains which data processors and third parties have access to the data, and how we protect the registered persons privacy.

1.2 Definitions

By registered person, registrant or user we mean the person the data concerns. This could be an employee, a field worker, a user of our services, a donor or a newsletter subscriber. In general this includes all persons we process and store data about.

Personal data is information that can be linked to and identify a person, for example name, address, date of birth, social security number, tax number or other personal identification numbers, telephone number, photo, e-mail address and IP-address.

Processing of personal data includes any use of personal data for example for the purpose of fundraising, registration, assembly, storage and extradition, or a combination of such uses. All processing of personal data is governed by the personal data regulation applicable at any given time.

A data controller is in charge of overseeing that these regulations are complied with at all times. A company or an organisation is considered to be responsible for the data processing upon determining the purpose of processing data and how to use it. The organisation remains responsible even if a third-party data processor, as for example a system supplier, authorities or accountants, is involved. The organisation is responsible for making the data processors understand that the organisation's regulations apply. More information on this subject under section 3.4.

2. Rights

2.1. Right of access (GDPR Article 15)
The registrant has the right to have insight into the data we store about him/her. Anyone requiring to access this data can send an e-mail to post@drapenihavet.no and mark the e-mail with "Personal Data Insight". The request will be handled by our data controller and the response will be available within one month after the e-mail has been received (GDPR Article 12). If it is not possible to process the request within this deadline, information about this will be given within one month from receiving the e-mail.

2.2 Right to erasure (GDPR article 17)
According to the legislation, the registrant has the right to demand deletion of his/her personal data. This is called the right to erasure/right to be forgotten. The registrant may require that information is deleted when;

a. it is no longer necessary to keep the information in order to achieve the purpose of the processing
b. the processing is based on consent and the consent is withdrawn
c. the registered person has the right to oppose the processing of personal data
d. personal information has been processed in violation of the rules
e. personal data has been collected in connection with children's use of online services

DIH may, for statistical purposes, continue to store certain data on the basis of Article 89 of the GDPR. The following information can be stored after deletion of other personal data:

About field workers:
Gender, age, nationality, location and period for field work

About financial donors:
Gender, age, zip code/post code, donated amount, month/year of donation

About service users:
Gender, age, nationality, location

Personal data may be processed on the basis of Article 6 (1) (e) of the Privacy Regulation if it is necessary for archival purposes in the public interest, purposes related to scientific or historical research or statistical purposes, although it is no longer necessary for its original purpose. The processing shall be covered by the necessary guarantees in accordance with Article 89 (1) of the Personal Data Protection Ordinance.
In accordance with Article 89 (1) of the GDPR, technical and organisational measures must be implemented to ensure that the principle of data minimisation is compliable with the legislation. DIH ensures that the remaining stored data will be anonymised and/or encrypted. The information will only be processed to document the organisations activities to the tax authorities, public bodies, etc. in connection with application processes, data processing and situations where it is required to account for the organisations work and results.

Special categories of personal data
Processing of personal data of a racial or ethnic origin, political opinion, religion, belief or union membership, as well as the processing of genetic data and biometric data for the purpose of unambiguously identifying an actual person, his/her health information, sexual relationship or sexual orientation, is prohibited under Article 9 of the GDPR.

However, this prohibition is exempted (Article 9 (2) (j)), for statistical purposes. The prerequisites are that the processing takes place in accordance with Article 89, paragraph 1, on the basis of union law or the national law of the member states which must be proportionate to the objective sought, be consistent with the fundamental content of the right to protection of personal data and ensure appropriate and special measures to protect the registered persons fundamental rights and interests. That means that if a registrant wishes to delete all his/her information, personal data may still be processed without the consent, if the processing is necessary for archival purposes in the public interest, scientific or historical research, statistical purposes, and if the interest of the community clearly outweighs any disadvantages for the registrant. In case of a disagreement on this, a complaint can be made. See below in section 2.6 on appeal.

Registrants who wish to have their personal data deleted can send an e-mail to post@drapenihavet.no and mark it "Deletion of personal data". The request will be handled by our data controller and the replied upon within one month after the e-mail has been received. If it is not possible to process the request within this deadline, information will be given within one month after receiving the request. DIH will, upon request from the registered person regards deletion of personal data, send a confirmation that the information that identifies the person has been deleted, as well as feedback on which information is required to be kept.

2.3. The right to claim restriction (GDPR Articles 18 and 19)
If the registrant does not want information to be deleted or contest that the information is correct, he or she may require the processing of personal data to be limited. By limitation means that the information is stored and can only be used:

a. with the consent of the registrant,
b. in order to defend a legal claim,
c. to defend someone else's rights, or
d. to safeguard important social interests

When the information is to be deleted or restricted, the data controller is obliged to convey this to all who have received the personal data unless this is disproportionate or impossible.

2.4. The right to data portability (GDPR Article 20)
If someone processes personal data based on consent, for example, in order to fulfil an agreement with the registered person, the registrant may require to bring his information to another organisation. This is called data portability. If technically feasible, the registrant may require that the data controller ensures that the data is transferred to the new organisation. The information should be in a structured, widely used and machine-readable format. The right to data portability does not apply to processes that are necessary for carrying out tasks in the public interest or under public authority.

2.5. The right to oppose processing
Individuals have, in some cases, the right to object that their personal data is processed. All processing of personal data must have a processing objective. What valid processing objective entails is explained in GDPR Articles 6 and 9. Whether or not an individual can be exempt from data processing is dependent upon what the processing basis is or what the purpose is.

Individuals can be exempt if:

a. The data is processed because it is necessary to carry out a task in the public interest or for public authority issues according to the nature of the regulation. 6 (1) (e)

b. The data is processed on the basis of an interest analysis. 6 (1) (f)
c. The purpose of the processing is direct marketing (regardless of what the processing objective is)

If an individual opposes, the data controller must stop processing, and delete the personal data. Nevertheless, the data controller may continue to process the personal data if the organisation can show compelling, justified grounds outweighing an individuals' right to privacy (see also section 2.2). The same applies if processing is required to comply with a legal claim. This exception does not apply when the purpose is direct marketing. Then the individual is always entitled to oppose. Donors can decide what type of information or inquiries they wish to receive. By contacting giver@drapenihavet.no one can update consent or restrictions.

2.6. Right to appeal
Users/registered persons have the right to appeal to The Norwegian Data Protection Authority regarding the processing of his/her personal information, if they believe it has been done in violation of current privacy policy.

3. Personal data - processing and storage of these

3.1. Which data we collect, how and for what purpose?
Depending on what type of user the registered person is we collect information that is necessary for the organisation's work. Personal data will not be stored longer than necessary to fulfil the purpose of the processing. The purpose of processing/storing the different types of personal data depends on the type of commitment the registrant has in DIH, and is explained underneath.

Newsletter subscribers
We will store the e-mail address, first name and last name if the subscriber has provided this to us through our website. This is needed to send out the newsletter they have subscribed to.

Donors
We store information they have provided, such as name, address, e-mail address, phone number, date of birth, gender, and national identity number. The donor may give this information either directly to us or through their bank, Vipps, Paypal or mobile pay solution. Donors in Norway have the opportunity to provide their national identity number encrypted, in order to received tax deductions for their donation. This also goes for donations through Facebook.
The purpose of storage is to report to the tax authorities if the donor wants tax deductions, to ensure predictability, keep an overview of the organisation's financial situation and for statistics. We also need this to inform the donor about the importance and effect of their contributions. To ensure that the contact information and potential reservations are updated, our data controller will do regular checks against the Norwegian National Register (for registrants in Norway).

Field workers
We save the following data provided by the applicant when registering in our recruitment system and HR-system; name, gender, nationality, date of birth, address, e-mail, phone number, occupation, experience from humanitarian work. We need this in order to plan participation and to communicate with the candidate before, during and after the assignment.

We also store contact information to next of kin (name and telephone number), in case of an emergency situation. We store information about where the fieldworker has worked with us and what period he/she was at the location. Field workers provide the organisation with their criminal background check, insurance information and passport number or copy of passport. To maintain the security of the field worker we also collect data such as name, mobile number and geographical position (when the user has turned on this feature), as well as accommodation on the location, in our security system as long as the field worker is on duty. Data is also forwarded to local and national authorities where this is required.

Employees

Applications and CVs are stored in our recruitment system and HR-system together with name, address, e-mail and phone number. About employees we also store social security number, bank account number and work contract in our HR-system and accounting/payroll system. This data is provided to us by the employee before contract is signed and also provided by tax authorities, and is needed in order to set up contracts as well as having the employee enrolled in the pension- and insurance agreements of the organisation.

Service users

DIH provides a range of services and activities, both inside and outside refugee camps and settlements. To be able to provide fair distributions, optimized staffing, sufficient stock, purchase schedules as well as registering participants to activities we need to gain some data. About these participants we may store name, age, nationality and address/container number in the camp. The data is given to us by the participant themselves or by the representatives from the camp.

Webshop

Upon purchase in our webshop, the customer provides us with data such as name, address, e-mail address, phone number and products purchased, is saved. We need this to be able to send the shipment to the correct receiver.

3.2. Third parties and where information is stored

Personal data is processed by third party data processors in their databases, and required for us to monitor and perform our work. Data processing agreements have been made with relevant actors. DIH will not divulge, sell, convey or otherwise disclose personal data about the registrant other than what is stated in this Privacy Policy, unless we are required to do so as a result of a binding court decision or we have received the consent of the registrant. However, this does not prevent us from using a data processor that processes the personal information on our behalf in accordance with the data processing agreement. Data processors who gain access to personal data through their services for DIH, are subject to confidentiality and are not allowed to use this information in any other way than performing the services for us, as of the GDPR Article 28. All data processors we use have policies for processing personal data under GDPR.

Links to our system vendors / data vendors privacy policies:

Solidus: https://solidus.no/personvernerklaering/
Paypal: https://www.paypal.com/no/webapps/mpp/ua/privacy-full
Teamtailor: https://www.teamtailor.com/en/privacy-policy/
Huma: https://www.hu.ma/privacy-policy
Tripletex: https://www.tripletex.no/gdpr-og-personvern/

Gjensidige: https://www.gjensidige.no/personvern-og-sikkerhet
Skatteetaten: https://www.skatteetaten.no/om-skatteetaten/personvern/
DnB: https://www.dnb.no/om-oss/personvern.html
Amazon Web Services (AWS): https://aws.amazon.com/compliance/eu-data-protection/
Wordpress/WP Hotel: https://wphotell.unitedworks.no/vilkar-og-betingelser/
Stripe: https://stripe.com/en-no/privacy
Facebook: https://www.facebook.com/privacy/explanation
WhatsApp: https://www.whatsapp.com/legal/privacy-policy-eea
Vipps: https://www.vipps.no/vilkar/cookie-og-personvern
Mailchimp: https://mailchimp.com/legal/privacy/?_ga=2.55378347.1202434019.1528100659-579363101.1528100659
Microsoft: https://privacy.microsoft.com/nb-no/privacystatement
Trygg Global: https://www.tryggglobal.com/privacy-policy/
Google Cloud Services: https://policies.google.com/privacy?hl=en
Adstate: https://www.adstate.com/privacy-policy
Quickbooks: https://www.intuit.com/privacy/statement/
Boxtribute: https://www.boxtribute.org
Givepanel: https://givepanel.com/privacy/

4. Security and protection of personal information and routines

4.1. Routines and measures

We have routines and measures to avoid that unauthorized persons gain access to personal data and that processing is performed in accordance with applicable law. Measures include regular risk assessments, two-step verifications and procedures to verify inspection and deletion requests. We also have internal routines for approving new system vendors and software All users of DIH IT-systems must follow instructions for electronic communication describing how we protect and handle personal data and privacy. We have internal routines and measures in case of discrepancies in processing and storing of personal data.

4. 2 Use of analytics tools, cookies and other technologies

We continuously work to improve the user experience and the functionality on our website. For these reasons we collect data from our users. Examples of such data are which pages are visited, at what time and what kind of browser was used. By using our website, users agree that we may use such tools unless they disable them, by changing settings for cookies in their browser. Cookies are text file stored on the user's PC/mobile phone/tablet, which helps us make the visits to our websites more user friendly. Web applications that allow you to register a personal profile uses cookies to save user preferences in the browser. In your browser settings you can find an overview of cookies that are stored on your device and delete unwanted cookies.