# CHOICE's General Data Protection Regulation, Privacy Policy and Cyber Security Policy

**Chapters:**

## Introduction

In 2009, the European Union (EU) declared that everyone has the right to protect their personal data. In 2018, the EU law of General Data Protection Regulation (GDPR) went into effect. It aims to strengthen how data is protected, hold organizations more accountable for protecting people's data, and explain the rights of people to their data privacy.

GDPR, cyber security and data protection are of great importance for CHOICE for Youth and Sexuality (hereafter CHOICE). The focus of our work, sexual and reproductive health and rights (SRHR) for young people, is a sensitive and controversial topic. Therefore, it remains in the interest of CHOICE and the young people we serve to ensure our work, including data and information, and that of our programmatic partners, is secure.

Furthermore, there has been an increase in the number of cyberattacks directed at NGOs, and therefore, we must protect CHOICE from such attacks to prevent any negative publicity/attention or financial loss (from ransoms and bribes, lost data, and lost time).

CHOICE should have a GDPR policy, privacy policy and a cyber security policy. **The GDPR policy** *should prove that CHOICE abides by the GDPR when we process and use data*. Organizations must be able to prove they abide by the GDPR when they process personal data. By processing personal data this includes collecting, storing, using, forwarding, sharing, distributing, and merging data.

**A privacy policy** *should be drafted to tell people how we use their data and for how long we store it*. **A Cyber security policy** *should state how we protect our organization against threats and ensure cyber security at all levels*.

This document aims to collect *all* measures taken by CHOICE to abide by GDPR. The document will be organized in the following way; GDPR Policy, Privacy Policy, Cyber Security Policy.

Due to the nature of our work being focused on youth, this document aims to not only serve as a comprehensive proof of CHOICE's efforts to abide by GDPR, but also to provide this information in a youth-accessible manner for the sustainability of generations to come.

## Definitions and Acronyms

In this policy we will use the following terms. Please note that they are interrelated, not interchangeable.

Cyber Security: the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

Data Protection: legal control over access to and use of data stored in computers.

GDPR: General Data Protection Regulation. It is, "…the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU."

DPO: Data Protection Officer

OM: Office Manager

SRHR: Sexual, Reproductive Health and Rights

Personal data: any information which relates to individual humans. Including but not limited to health information or medical records, names, program reporting outlining an individual's trips or behaviors, photographs, videos, etc.

Sensitive personal data: GDPR defines some data separately as "sensitive" or "special category". This includes, but is not limited to, religions, race and ethnicity, information on health, sex life, sexual orientation, philosophical beliefs. It is illegal to process this data unless organizations take adequate steps to protect data security, as listed in the privacy policy.

Operating systems: is system software that manages computer hardware and software resources and provides common services for computer programs. For CHOICE, this refers to the Windows operating system on computers.

Back-end Organizations: for CHOICE, this refers to all systems, apps, and platforms CHOICE uses to run our internal organization. The biggest example would be Microsoft 365, as CHOICE's subscription to this platform allows access to SharePoint and an email account. This is where most of the work happens and is documented. This is also an example of a platform where our data is stored.

## General Data Protection Policy

The GDPR Article 5(1) has 6 principles as to how the act of collecting and processing data needs to be based upon:

1. **Lawfulness, fairness and transparency**
    I. It requires personal data to be processed in a lawful, fair and transparent manner. This ensures the data subject receives information on the identity of controllers and purposes of the processing of personal data.
2. **Purpose limitation**
    I. Personal data is to be collected only for specified, explicit and legitimate purposes. It is not allowed to process personal data in a way that is not compatible with those purposes.
3. **Data minimization**
    I. According to this principle, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy**
    I. It is required to ensure that personal data is accurate and kept up to date where necessary. Personal data that is inaccurate (considering the purposes for its processing) must be deleted or rectified without any delay.
5. **Storage limitation**
    I. Personal data must be kept in a form that makes it possible to identify data subjects for no longer than is necessary for the purposes of the processing.
6. **Integrity and confidentiality**
    I. The processing of personal data requires the assurance of appropriate security of personal data. This should include protection against unauthorized or unlawful processing, destruction and damage.

The following GDPR, Privacy and Cyber Security Policies have been based upon these principles.

### How We Keep Records and Data and Back-End Organizations

For CHOICE to be a streamlined organization we need to use operating systems and back-end organizations. Before we choose which operating systems to use CHOICE ensures that we come to an agreement on; why we need the system, how they each will be used and if they have a sufficient data policy to protect the data we put into these systems.

To check if they have a sufficient data policy, we can assume that large(r) organizations, such as Microsoft 365, wouldn't be able to operate in the EU if they were not GDPR compliant. As we are a small NGO with limited capacity, we do not have the resources or time to sift through these policies and ensure smaller organizations are compliant. We can rely on the privacy authorities to check. So, for smaller organizations, CHOICE defines a sufficient data policy as one with a GDPR and privacy policy.

Below is detailed the main systems we use, why we need them, how we use them and if they have a sufficient data policy to protect our data:

Before selecting operating systems for organizational use, CHOICE ensures alignment on the following key points: the specific need for each system, the intended use, and verification of each system's data protection policies to ensure adequate safeguarding of our data.

To assess the sufficiency of a system's data protection policy, we assume that larger organizations, such as Microsoft 365, meet GDPR compliance standards as they would otherwise be restricted from operating within the EU. Given our capacity constraints as a small NGO, CHOICE lacks the resources to conduct exhaustive compliance reviews of each policy individually, particularly for smaller providers. Instead, we rely on the oversight of relevant data protection authorities. For smaller providers, CHOICE defines a sufficient data policy as one that includes both GDPR compliance and a clearly stated privacy policy. For each system below, we conducted this check to determine the status.

Outlined below are the primary systems we utilize, the rationale for each, our usage approach, and the data protection policies in place to safeguard our data.

***Microsoft Office 365 (mainly SharePoint, Teams, and Outlook)***

Why we need it

When someone starts working at CHOICE, they receive access to our Microsoft Online 365 subscription. This gives them access, most notably, to an email address that is linked to our account, to our SharePoint, Teams, and Outlook. We specifically have the E2 version which provides a 2016 version of Microsoft applications at a lower price for NGOs.

The Office Manager (OM) has access to CHOICE's main Microsoft 365 account, which is the key user account. As a backup, access to this account can be provided to the chair of the board via the OM. In this account role, the OM can grant varying access to different profiles based on the level of access they require.

How we use it/any notes

CHOICErs use Microsoft 365 to access SharePoint which is where we store all our work. According to the assigned profile, they will be given varying access to SharePoint. For example, Youth Advocates have limited access and when they work on projects with staff, they must request the OM to share the relevant folders with them. Another example is that the finance folder is shared only with those on the finance team.

Every CHOICEr is required to have Multi-Factor Authentication enabled in order to add an additional layer of security before accessing CHOICE's online data.The OM also heavily uses Microsoft 365/SharePoint to store personal data of CHOICErs. See “Data on file of CHOICErs and ex-CHOICErs".

Sufficient data policy based on the above guidelines?

Yes.

***Barracuda Backups***

Why we need it

Barracuda Backups provides cloud back-up services for the Microsoft Office 365 suite. The backup is made once a day automatically by the software. Helpful when/if data is accidentally or deliberately lost.

How we use it/any notes

The OM has access to the Barracuda Backups services. Only use it when our data is accidentally lost, e.g. someone accidentally deletes something off SharePoint, the OM can restore it. This occurs only on a needs basis.

Sufficient data policy based on the above guidelines?

Yes

***Violet88 and Savvii***

Why we need it

We use Violet88 and Savvii to host our website. They are back-end website experts which we use as CHOICE does not have the capacity to hire our own website developer/train our communications manager to learn website development. In our contract with them, we lay

out clear rules for the treatment and usage of any private data that may be used to develop and maintain our website.

How we use it/any notes

They simplify our online presence by streamlining the back-end work for us.

Sufficient data policy based on the above guidelines?

Yes

***Diversity Travel***

Why we need it

Diversity Travel streamlines the process of making bookings, comparing prices, holding quotes, while still ensuring the proper approval processes are set up.

How we use it/any notes

We use Diversity Travel to compare prices for our bookings when we travel. They provide private agents and an online system which shows different prices and fares on tickets for travel. They also can hold quotes for us while we discuss. They can also help in emergency situations if a staff member needs to leave the country quickly.

Sufficient data policy based on the above guidelines?

Yes. They also have access to everyone's passports who uses the site, which is used to streamline booking processes and make necessary modifications to travel arrangements.

***Exact Online***

Why we need it

We use Exact Online as our online accounting system. Streamlines Profit and Loss statements and our accountants monthly and annual work.

How we use it/any notes

The OM and financial accountant are the main users.

Sufficient data policy based on the above guidelines?

Yes.

***ABN AMRO Online Banking***

Why we need it

Used by the finance team to manage banking. Mainly sending out payments.

How we use it/any notes

There are different levels of access granted according to people's roles. For example, the ED cannot prepare payments but can only approve them, on the contrary the OM can only prepare payments but not approve them. Please see the xxx policy for more information.

Sufficient data policy based on the above guidelines?

Yes.

***Promeva***

Why we need it

Use this for monthly reporting of programs as part of the planning, monitoring, evaluation and learning process. It is a part of the system used to track progress within the programs and helps determine how well a program is functioning. Promeva is a commonly used platform in the international development sector, and one that has established GDPR-compliant processes

How we use it/any notes

Programmatic workers will monthly fill out the online system with data from our programs.

Sufficient data policy based on the above guidelines?

Yes.

***Google Drive***

Why we need it

Some partner organizations we work with do not use similar systems like SharePoint/Microsoft Office 365, as they require more funding. Therefore, sometimes staff will need to use Google Drive to co-work with partner organizations.

How we use it/any notes

With partner organizations so we can all co-work on documents together.

Sufficient data policy based on the above guidelines?

Not as enough as Microsoft 365, but sometimes we must adapt to other situations. When there are more data sensitive topics, staff will use Microsoft 365 and Outlook to discuss in order to ensure encryption through Multi-Factor Authentication.

***Other operating systems we use on smaller scales:***

- Mentimeter
    - For making presentations
- Kahoot
    - For making fun games
- Buzzsprout
    - For our podcast
- WhatsApp
    - For communicating at all CHOICE levels
- Zoom
    - For meetings outside of Teams. Zoom sometimes uses AI bots, staff has discussed this and decided we will turn this off.
    - Sometimes staff will provide access to our zoom account to people we work with if they cannot access Zoom themselves. We do ask them to sign out afterwards. The passwords are then circulated afterwards.
- Meta products such as Facebook and Instagram
    - For social media and communications material to showcase CHOICE in the public domain
- TikTok
    - For social media and communications material to showcase CHOICE in the public domain
- LinkedIn
    - For social media and communications material to showcase CHOICE in the public domain

**The DPO's Role and our Organization**

The GDPR states that the decisive factor of whether to have a DPO or not is based on the core processing activities that are essential to achieving the company's goals, rather than the size of the organization.

For example, a company could be large but not process sensitive personal data, so it would not need to appoint a DPO. However, if a company *does* process sensitive personal data, as it is essential to the organization's goals, then they should appoint a DPO.

According to article 37 of the GDPR a Data Protection Officer (DPO) is necessary when 1) the processing is carried out by a public authority or body, 2) the core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, or 3) the core activities of the controller or the processor consist of processing special categories of personal data or data relating to criminal convictions and offences.

These cases do not apply to CHOICE. However, since CHOICE does deal with sensitive personal data to complete our organization's goals (such as applying field data of peoples at UN reports, or generally sexual, reproductive, health and rights), CHOICE chooses to appoint a DPO.

Below is an overview of GDPR aspects and which individuals within CHOICE are responsible for monitoring compliance within our work. Within the Privacy Policy chapter there is a more in-depth breakdown of what specific data is collected and why.

| **GDPR Aspect** | **Responsible** | **Notes** |
|---|---|---|
| DPO | Office Manager | It must be noted that the DPO's role is as an advisory council to the board and organization. They shall not be held legally accountable if it is found that CHOICE is not complying with GDPR law. |
| Processing personal data of staff members | Office Manager, Executive Director and Chair of the Board | All 3 individuals work together to process relevant staff data. More on this breakdown of what is considered relevant staff data within the Privacy Policy chapter.<br>For example, the Office Manager processes travel documents and addresses, but not salaries and pay slips. |
| Processing personal data of board members internally | Office Manager | This relates to travel documents, and addresses. |

| | | |
|---|---|---|
| Processing personal data of board members externally | Chair and Treasurer of the Board<br>Sometimes the Office Manager | This relates to registrations at the Chamber of Commerce<br>Every now and then, the Office Manager will also help with this. |
| Processing personal data of Youth Advocates | Office Manager | |
| Certificate of Good Conduct/VOG | Office Manager and Executive Director and Chair of the Board | Staff, Financial Accountant and Board members are all required to provide a certificate of good conduct. This is process mainly by the OM and relevant individual but also is sometimes needed to be access by the Executive Director and Chair of the Board |
| Processing personal data of applicants | Selection Committee and Office Manager | The Selection Committee for the position will process applicant's data. The Office Manager will ensure it is erased after the selection process is finalized. |
| Processing personal data of Partner Organizations | Program Coordinators and Executive Director | |
| Signing Data Processing Agreements with third parties | Executive Director | |
| Data Leak Procedure | Office Manager/DPO, Chair of Board and any relevant involved individuals | The DPO works with the Chair of the Board and the relevant involved individuals to take the necessary steps to prepare in case of a data leak/to follow said steps. Read more about this in the Cyber Security Chapter |
| Annual Checks and Risk and Gap Analysis | Office Manager/DPO, Chair of Board | The DPO (the OM) will lead on this, but advise the Chair of the board |
| Processing data from survey respondents and online consultations | Relevant staff members | |

**Annual Plan: Check and Audit, and Risk and Gap Analysis**

Within CHOICE's steps to comply with GDPR, there are annual activities that should be followed. These include an annual plan, checks and internal GDPR audits.

Annual Plan

Below is a table which lays out what GDPR activity happens throughout the year at CHOICE. These are all led by the DPO, but if needed, the DPO can rely on the Chair of the Board (e.g. sickness or low capacity).

| **What** | **When** |
|---|---|
| Risk and Gap Analysis | October |
| Check and Audit | November |
| Fake phishing email | Randomized every year to ensure the surprise factor |
| Annual refresher for CHOICErs | When a new CHOICEr joins, they will have to take a mandatory introduction to GDPR at CHOICE. This will take place most often in March as new Youth Advocates join in February and have onboarding sessions from there onwards. After completing this course, they will be asked to sign the Privacy Policy.<br><br>To ensure that knowledge is refreshed and updated, CHOICErs who have already taken the mandatory course will be given a small quiz. If they pass the quiz with 80% or above, then they do not have to re-attend the mandatory refresher session. Once a CHOICEr has gone 2 years without taking the session, they are required to sit the session again. |

GDPR Annual Check and Audit

Within the annual check audit, the DPO will review the GDPR policy. During this review, the DPO shall see if there is anything that needs to be updated. This will be based on any relevant developments in GDPR law, cyber security recommendations and CHOICE's Risk and Gap Analysis.

The DPO will also work on writing a report which details the steps that year that CHOICE has taken to comply (on top of this plan/policies). The report will also include relevant next steps to take that year based on the Risk and Gap Analysis.

Risk and Gap Analysis

The Risk and Gap Analysis is an analysis that the DPO organizes every year. This analysis is a check to identify and evaluate the current state of our system and process and compare it to the desired state. The end goal is to identify the areas and gaps of non-compliance that need to be met within our policies, procedures and practices.

Throughout this analysis the DPO reviews the previous year for any threats that were prominent or recurrent, any gaps with where CHOICE currently stands and then any (prioritized) future steps for CHOICE to focus on in the coming year.

**Always Know Your Rights, But It's Our Job to Tell You**

A large part of GDPR compliance is the responsibility of CHOICE to ensure that all CHOICERs and people who work with CHOICE are aware of their rights regarding the privacy, protection and use of their personal data. Below, we outline the relevant Articles within the GDPR which are about the rights of stakeholders. Below each article, is a "translation" in which the article is rewritten in a more accessible manner. If you have any questions, please feel free to contact the DPO (the Office Manager). This is also covered in the mandatory GDPR introduction session.

Article 15: Subject Access Requests

Staff, donors, external parties, people we work with, and volunteers all have a right to obtain any personal data relating to them that CHOICE holds. GDPR calls this a subject access request.

Article 15 states:

"1. The data subject shall have the 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 and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;

- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others."

Translated in a more human/accessible manner:

1. You have the right to inquire whether or not your data is being processed. If it is, you are allowed to know/ask for:
    a. Why it is being processed
    b. The categories of which personal data is being processed
    c. The recipients who can access the personal data/will have the personal data shared with them. Even if this is in third countries or international organizations.
    d. The expected period for how long the data is being stored. If this is impossible, the criteria used to determine that period.
    e. Your right to request rectification, erasure or restriction (of processing) your personal data. You also have the right to object to the processing.
    f. The right to lodge a complaint with a supervisory authority.
    g. If personal data is not collected from the source itself, any information as to the source it was derived from.
    h. If automated decision-making exists, including profiling referred to in Article 22(1) and (4). In cases where it does exist, meaningful information about the logic involved, significance and the consequences of processing for the subject.

2. If personal data is transferred to a third country or an international organization, you have the right to be informed of safeguarding practices for the transfer of this data.
3. The administrator/controller can provide you with a copy of your personal data which is being used in processing. For further copies, we have the right to charge a reasonable fee due to administration costs. If you request this electronically, you can request physical copies of your data, but if you do not specify, we can provide you with the information in a commonly used electronic form.
4. The right to obtain a copy of your data in nr. 3 should not affect the rights and freedoms of anyone else.

We have 30 days to fulfil your request. If you receive a request from someone, please notify us immediately!

Article 17: The Right to be Forgotten

Also known as the Right to Erasure, Article 17 of the GDPR allows users to obtain from data controllers the erasure of their personal data.

Article 17 states:

"1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defense of legal claims."

Translated in a more human/accessible manner:

1. You have the right to obtain from the controller the erasure of personal data concerning you. This should be without a substantial delay. The controller should also erase your data without delay when the following applies:
    a. Your personal data is no longer necessary for the purposes for which we collected and processed them
    b. You withdraw consent on which the processing is based on point a of Article 6(1) or point a of Article 9(2)
    c. You object to processing in line with Article 21(1), if there are no overriding legitimate grounds for processing, or you object to the processing in line with Article 21(2)
    d. Your personal data has been unlawfully processed
    e. Your personal data must be erased to comply with a legal obligation in Union or Member State law to which you are under subject
    f. Your personal data has been collected in relation to the offer of information society services referred to in Article 8(1)

2. When we have made the personal data public and are required to erase the personal data according to paragraph 1, (within reason of technology available and costs) we have to take reasonable steps to inform whoever has this data or is processing it that it has to be erased. Including copies or replications.
3. Paragraphs 1 and 2 do not apply if the processing is necessary:
    a. To exercise the right of freedom of expression and information
    b. To comply with legal obligations which require processing by Union or Member State law for the controller to perform a task in public interest or exercise official authority vested in the controller
    c. For reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) and Article 9(3)
    d. To achieve purposes in public interest, scientific, or historical research, statistical research purposes in accordance with Article 89(1). As long as the right referred to in paragraph 1 is likely to seriously impede the achievement of the objectives of that processing
    e. For the establishment, exercise or defense of legal claims.

# Privacy Policy

A privacy policy should be drafted to tell people how we use their data and for how long we store it.

## Data on File/What Data We Use/How Long We Keep Data

CHOICE processes personal data from its board members, staff members, youth advocates, partners, donors, applicants, third parties, respondents to surveys, and external persons, and persons who had a previous working/volunteering relationship with CHOICE. This section describes per group what personal data are being collected, how these personal data are being processed, for which purposes, and how long these data are being stored.

A note on youth friendliness: As CHOICE is youth-led, many CHOICErs do not have previous knowledge capital about systems that we consistently use (for example the Chamber of Commerce or setting up our banking information). Therefore, sometimes it is important that although a CHOICEr has left, we ensure that some of their data or information stays within the organization. This way, we are trying to avoid the steep learning curve.

### Board

From its board members CHOICE gathers personal data for the following purposes:

- Fulfillment of the contract;
- Registration at the Chamber of Commerce;
- (Financial) administrative purposes;
- Communication purposes;
- Travels abroad;
- Sharing information.

There are three legal foundations for processing personal data of board members. First, the processing of the board members' personal data is necessary for the fulfillment of the contract. Second, the board members have given consent to the processing of their personal data. Finally, it is necessary in order to comply with a legal obligation.

CHOICE gathers the following personal data from their board members:

- Name;

- Address;
- Zip code;
- Phone number;
- E-mail address;
- Date of birth;
- Bank details;
- Passport copy;
- Contact details (name + phone number) of one relative to contact in case of emergency.

The above-mentioned personal data are collected by the Chair of the Board and the Office Manager (OM) through e-mail. The passport copy is stored in a secure folder on SharePoint, which can only be accessed by the ED and the OM. The bank details are not separately stored on SharePoint, but are on the reimbursement forms that board members hand in. These are only accessible for the Chair, Treasurer, the ED, the OM, and the Financial Controller. All other personal data is stored in folders accessible for all CHOICE members (board, staff and Youth Advocates).

Board members sign a contract and register at the Chamber of Commerce. Therefore, before the start of their work, board members sign a separate document where they give consent for their personal data to be processed and where they declare to process the personal data of staff members only in compliance with the GDPR.

Board members are responsible for keeping their personal data up to date and should contact the OM in case of any changes. The personal data is stored for the duration of the contract and a maximum of two years after termination of the contract. The OM is responsible for deleting personal data from board members within this determined period. The CHOICE email account of the leaving board member will be deleted by the OM after three months after termination of the contract. The reimbursements have to be stored for 7 years according to Dutch law.

Youth Advocates

From its Youth Advocates (YA's), CHOICE collects personal data for the following purposes:

- Fulfillment of the volunteer contract;
- (Financial) administrative purposes;
- Communication purposes;

- Travels abroad;
- Sharing information.

There are two legal foundations for gathering personal data from YA's. First, the processing is necessary for the fulfillment of the volunteer contract. Second, the YA's have given consent to the processing of their personal data.

The personal data that CHOICE gathers from Youth Advocates are as follows:

- Name;
- Address;
- Zip code;
- Phone number;
- E-mail address;
- Date of birth;
- Bank details;
- Passport copy;
- Contact details (name + phone number) of one relative to contact in case of emergency.

The above-mentioned personal data, except for the bank details, are collected though the volunteer contract. By signing the contract, YA's give consent for their data to be processed. After signing the volunteer contract, the OM is responsible for processing the personal data. The passport copy is stored in a secure folder on SharePoint, which can only be accessed by the ED and the OM. The bank details are not separately stored on SharePoint, but are on the reimbursement forms that staff members hand in. These are only accessible for the Chair, the Treasurer, the ED, the OM and the Financial Controller. All other personal data is stored in folders accessible for all CHOICE members (board, staff and Youth Advocates).

YAs are responsible for keeping their personal data up to date and should contact the OM in case of any changes. The personal data are stored for the duration of the volunteer contract and a maximum of three months after termination of the contract. The OM is responsible for deleting the YA's personal data within this determined period. The CHOICE email account of the YA will be deleted by the OM after three months after termination of the volunteer contract. The reimbursements have to be stored for 7 years according to Dutch law.

Staff

From its staff members, CHOICE collects personal data for the following purposes:

- Fulfillment of labor contract;
- (Financial) administrative purposes;
- Personnel administration;
- Salary administration;
- To comply with the tax law;
- Communication purposes;
- Travels abroad;

Sharing information.

There are three legal foundations for processing personal data of staff members. First, the processing is necessary for the fulfillment of the contract. Second, the staff members have given consent to the processing of their personal data. Finally, the processing of the emergency contact details is necessary in order to comply with the law.

CHOICE processes the following personal data of staff members:

- Name;
- Address;
- Zip code;
- Phone number;
- E-mail address;
- Date of birth;
- Bank details;
- Passport copy;
- Salary;
- Citizen Service Number;
- Personnel file;
- Leave/medical file
- Contact details (name + phone number) of two people to contact in case of emergency.

All the above-mentioned personal data are sent to the ED by the new staff member before the start of the labor contract. All data is stored and processed in the personnel file, the leave/medical files or the salary administration. The personnel file and leave/medical files are only accessible for the ED. The salary administration and contracts are accessible for the Chair, Secretary, Treasurer and the ED. The hardcopy personnel files are stored at the

office. The ED is responsible for the correct processing of the personal data of the staff members.

Furthermore, the bank details are also accessible for the Chair, the Secretary, the Treasurer, the OM and the Financial Controller because it's on the reimbursement forms that staff members hand in. The passport copy is stored in a secure folder on SharePoint, which can only be accessed by the ED and the OM. Name, address, zip code, phone number, date of birth and contact details of the emergency contacts are stored in folders accessible for all CHOICE members. A hard copy of the emergency contact details is also stored in the office.

Staff members are responsible for keeping their personal data up to date and should inform the ED in case of any changes. The OM is responsible for keeping addresses, phone numbers and contact details of emergency contacts up to date. The labor contract and the personnel file will be stored for the duration of the contract and two years after termination of the contract. The other personal data will be stored for the duration of the contract and seven years after termination of the contract, as the law requires.

After termination of the contract of a staff member, the password of their e-mail account will be changed after 2 weeks. The e-mail account will be available for the successor and team members for another 6 months. After 6 months the e-mail account will be deleted by the OM.

Partner organizations

From its partner organizations, CHOICE collects the following information:

- Name;
- Address;
- Zip code;
- Phone number;
- E-mail address;
- Bank details;
- Registration details;
- Name and e-mail contact persons;
- Contract of partnership;
- Working documents e.g. year plan, year budget, (bi-)annual narrative and financial reports.

There are two legal foundations for processing personal data of partner organizations. First, relevant organizational documents are necessary for CHOICE and partner organizations for the due diligence and contract. These are part of the donor requirements. Second, by signing the contract the partner organization agrees with processing this information.

All the above information will be processed by the Program Coordinators and stored under the partner folders in SharePoint. These are accessible for the Board, Staff and Youth Advocates.

CHOICE will store these data for the duration of the partnership, and up to seven years after termination of the contract as this is required by Dutch Law. After this period, the personal data will be deleted by the OM and other information will be stored in the partner archive. The OM will annually check the archive on the expiration date.

### Third parties

CHOICE works with several parties that process personal data of CHOICE members. These parties include:

- Salary administration company
- Health and Safety Service (Arbodienst)
- Financial officer
- IT support
- Travel agency
- Internet and phone provider
- Printer company
- Website host company
- Contractors such as consultants, trainers, designers etc.

Where the processing has to be carried out, CHOICE makes sure to ensure the protection of the rights of the data subjects. This means that the processing of personal data is not being carried out without a governing contract, the Data Processing Agreement. CHOICE has a standard contract in place that is adjusted for every party. This standard Data Processing Agreement can be found in Annex II.

To communicate about the orders that we give to the above-mentioned parties, and for the fulfillment of the contract and administrative purposes, CHOICE processes the following personal data of these parties:

- Name (first name + surname)
- (Business) phone number
- (Business) e-mail address
- Bank details

This personal data is stored for the duration of the contract and a maximum of seven years after termination of the contract.

### Travel agency

To book the travel for CHOICERs, CHOICE uses the ATPI travel agency. On ATPI's website the OM creates an e-profile for the staff member or Youth Advocate who is planning to travel for a work trip. These e-profiles include the following personal data:

- Name (first name + surname)
- Emergency contact details (name + telephone number)
- Primary passport details:
- Gender as indicated on the passport
- Date of birth
- Passport number
- Passport expiry date
- Country of issue
- Citizenship

There are two legal foundations for processing personal data of staff members as such. First, the processing is necessary for the fulfillment of the contract, as without travel aboard, the staff members cannot do their work. Second, the CHOICERs have given consent to the processing of their personal data.

The e-profiles of staff members will be deleted manually by the OM if they have not been used for 6 months. The profiles of Youth Advocates or board members will be deleted three months after they have returned from their travel for CHOICE. Furthermore, when a CHOICEr leaves, their e-profile will be deleted three months after they have left.

### Relations

CHOICE furthermore processes contact details of relations, partners and interested people, who have given their consent for this, for communication and relationship

management purposes.  This can include people who have subscribed to our newsletter or people who have given permission to keep their contact details so that we can invite them to events. The legal foundation for processing this personal data is that these relations have given their consent.

### Applicants

CHOICE receives open applications in the general e-mail inbox (info@choiceforyouth.org) and applications for specific positions during outstanding vacancies in the vacancies inbox (vacancies@choiceforyouth.org). These e-mails contain resumes and motivation letters with personal data. CHOICE will not process the personal data of open applicants. When a person sends an open application, the OM will respond that we do not keep open applications in file. The OM is responsible for responding to open applicants and deleting their personal data within two weeks after receiving the e-mail.

In case of applications for a specific position, the personal data of the applicant is only accessible by the selection committee and the OM. The personal data of the applicant will be stored for the duration of the application procedure and a maximum of four weeks after the end of the selection procedure. The OM is responsible for notifying the applicants about the saving and termination process and for deleting their personal data within time. The standard timeframe used for this is 2 weeks after the vacancy has been completed. By completed, this refers to a candidate signing their contract. Until then, CHOICE keeps the applicant's data in case they are chosen.

### Survey respondents

CHOICE conducts surveys in order to ensure evidence-based interventions and advocacy. Before sending these surveys, CHOICE must include a section for the respondents which describes what the intent of the data collection is for.

For these purposes CHOICE may gather special categories of personal data, such as data concerning health or data concerning a person's sex life or sexual orientation. To protect and respect the privacy of the survey respondents, CHOICE only processes (special categories of) personal data with the explicit consent of the data subject. Furthermore, CHOICE makes sure to only gather and process personal data that are necessary for the above-mentioned purposes. The personal data of the data subjects should only be accessible for the person(s) conducting the research of the survey, and should be permanently erased after researching the data for the purpose of the survey.

Partnership requests

CHOICE regularly receives e-mails in its general mailbox info@choiceforyouth.org from organizations from all over the world, with the request to become a partner of CHOICE. CHOICE is currently not looking for a partner but considering the future it is interesting to keep those requests on file for a determined period. Therefore, CHOICE will ask for permission to keep the organization concerned in file for 2 years. If the organization gives permission, then the partnership request will be kept in a folder in the mailbox. If the organization does not give permission, then the partnership request will be deleted. The OM will check each quarter.

Website contact forms

CHOICE frequently receives filled out forms through their contact form on the website, which is filled out by people who have specific questions for us or want to have contact with us. People are asked to fill out their name, phone number and mail addresses. Hence, these contact forms contain personal data. The OM is responsible for responding to them by mail and deleting their personal data within two weeks after reception of the e-mail.

Record of processing activities

CHOICE has a record of processing activities to keep track of the processing of personal data. This Excel document records the categories of data subjects, the types of personal data, the legal foundations, the purposes of processing, the storage term, the responsible for processing, the processing by third parties, and the storage place.

**Physical Copies of Information/Data on Computers**

CHOICE staff are given computers when they join. When they leave, they are asked to wipe all personal information, upload any relevant information to SharePoint for other staff to access. They can transfer any personal and/or relevant documentation to their personal accounts. They then hand in their computers and the OM wipes/clears the personnel's computer account deleting all files, sign ins, etc.

The CHOICErs are asked to also sift through physical copies of information (printed files, etc.). If there is anything relevant to keep, they will hand it over to another CHOICEr. Files

which can be thrown away with no sensitive data are recycled. Files which have sensitive data need to be thrown away in the office's shredder and/or the recycling bin in the office building which is locked and only opened when the recycling center is reached.

There is also sensitive data in the office, locked every night, and the only people with access are the cleaners, building managers and staff.

## Cyber Security Policy

Cyber security policy should state how we protect our organization against threats and ensure cyber security at all levels.

### How Do We Ensure Protection?

CHOICE currently does the following to improve cyber security:

- When there is a new CHOICEr they must follow a mandatory GDPR compliance, privacy and cyber security policy introduction session
    - If a CHOICEr has already taken this session, then before the session is given the following year to new CHOICERs, they must take a quiz. If they score 80% or higher, then they are allowed to not attend the session. The following year, if they score 80% or higher again, they are allowed to not attend the session.

However, after 2 years of not attending the session, they must attend the next session.

- CHOICERs inform the DPO if they are receiving regular spam/phishing emails that seem to follow the same format. The DPO informs CHOICERs on how to handle.
- Multi Factor Authentication is required for CHOICERs Microsoft 365 accounts.
- CHOICE uses Barracuda Backup in case anything is lost, or our accounts are hacked
- Password Policy: When a CHOICEr joins, the OM sets up their email address along with a password. Upon first logging in, the new CHOICEr is required to change their password. The following password criteria should be followed:
    - Passwords expire after 90 days. Users are notified 30 days before expiration.
    - Passwords must be at least eight characters long.
    - Passwords can have a maximum of 16 characters.
    - Passwords can't contain the user's account name or parts of the user's full name that exceed two consecutive characters.
    - Passwords must contain characters from three of the following four categories:
        - Uppercase letters (A through Z)
        - Lowercase letters (a through z)
        - Numbers (0 through 9)
        - The following non-alphabetic characters: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /
- We encourage everyone to follow regular updates for CHOICE devices as they cannot be centrally updated.
- As stated above in the GDPR Policy (underneath Annual Plan), CHOICE follows a regular Annual Plan which includes a Risk and Gap Analysis, a Check and Audit, and a fake phishing email to check user's compliance.

**What To Do in an Emergency Loss Situation/Limited Options of Protecting Data**

It is important for CHOICE to have an action plan in the case of an emergency loss situation, a data leak situation or when there are limited options for protecting data.

Data Leak Situations

Data leakage is when data is accidentally exposed to the public outside of our organization. It means that data that CHOICE collects is released when it should not be.

Examples include; losing a laptop resulting in access to CHOICE's operating systems, losing papers that contain non-encrypted personal data, losing a USB, emailing personal data to the wrong person, data being stolen in a cyber-attack, etc. When these situations happen, CHOICE has an obligation to record what happened and the steps that were taken afterwards. CHOICE must be able to prove that we took proper steps to counter these attacks, and if relevant, inform the relevant parties.

Depending on the situation, there is also a responsibility to report to the person whose data has been involved in the data leak, especially if it has serious consequences for their rights and freedoms. This is known as a personal data breach. The GDPR defines a "personal data breach" in Article 4(12) as: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

As required in Article 33(1), "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours (about 3 days) after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, 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 supervisory authority, Autoriteit Persoonsgegevens (AP), is not made within 72 hours (about 3 days), it shall be accompanied by reasons for the delay.

Translated into a more human/accessible manner: if there is a data breach which falls under the personal data breach definition above, the DPO should be notified in 72 hours (about 3 days) of the person becoming aware of the data breach. Unless it is unlikely to result in a risk to the rights and freedoms of natural persons (e.g. no need to send the DPO spam emails). The DPO should work with the person who flagged the data breach to notify the relevant parties of what happened, what data (as exact as possible) has been breached, and what future steps will be taken.

Any action which would lead to sever implications, the Chair of the Board, DPO and relevant CHOICEr will ensure to file a police report and inform the organization's insurance.

Data leaks action steps

| **Type of data leaked** | **Action Steps** |
|---|---|
| Spam Emails | Mark as spam/junk, delete and block sender. |

| | |
|---|---|
| | No need to inform the DPO unless you are receiving the same spam/junk email repetitively (either from the same sender despite blocking, or the same format of an email despite blocking). |
| Phishing Emails | Do not click on a link if you receive an email which looks odd.<br>Mark as spam/junk, delete and block sender.<br>No need to inform the DPO unless you are receiving the same spam/junk email repetitively (either from the same sender despite blocking, or the same format of an email despite blocking). |
| Account hacked/data leaked | Notify DPO of hacking/leaking within 72 hours (about 3 days), unless it is unlikely to result in a risk to the rights and freedoms of natural persons.<br>DPO calls with the person to discuss a recollection of how this happened, what was lost.<br>DPO informs Board member, and all have a call together to discuss next steps.<br>The DPO should work with the person who flagged the data breach to notify the relevant parties of what happened, what data (as exact as possible) has been breached, and what future steps will be taken.<br>It will be required to change all the user's passwords. This includes any account that has been used on the computer. The user will also be required to clear cache and history. |
| Theft in a public space/computer left behind in a public space/stolen | Notify DPO immediately.<br>DPO informs Chair of Board. DPO, Chair and user get together to write a report. Also, file a police report.<br>It will be required to change all the user's passwords. This includes any account used on the computer.<br>CHOICErs are informed that if they are using their work computer, or personal computer but for work, in a public space they should always lock their computer before going to the bathroom/going for a break/etc. This may also include automatic lock settings after a fixed period of time (e.g., five minutes). Also to make sure to only leave it in eye's view/with a trusted person. |

| | |
|---|---|
| Physical papers containing data left in a public space | All papers that are printed should also be stored on a computer's desktop or SharePoint so that no data is permanently lost.<br>Notify DPO within 72 hours (about 3 days), unless it is unlikely to result in a risk to the rights and freedoms of natural persons.<br>DPO calls with the person to discuss a recollection of how this happened, what was lost.<br>DPO informs Board member, and all have a call together to discuss next steps.<br>The DPO should work with the person who flagged the data breach to notify the relevant parties of what happened, what data (as exact as possible) has been breached, and what future steps will be taken.<br>The next steps depend on what kind of information has been lost, but will include notifying concerned individuals and update the steps in this document with learning for future such incidents. |
| CHOICE's Microsoft Account is hacked/data leaked | Notify DPO immediately.<br>DPO calls with the person to discuss a recollection of how this happened, what was lost.<br>DPO informs Board member, and all have a call together to discuss next steps.<br>The DPO should work with the person who flagged the data breach to notify the relevant parties of what happened, what data (as exact as possible) has been breached, and what future steps will be taken.<br>Everyone in the organization will be required to change all of their passwords related to CHOICE.<br>If our data is leaked, we will need to write a comprehensive report about what sensitive information has been lost and the possible consequences. |
| Office burns down, or another situation where both physical and digital data is lost | Notify DPO, all board members, and ED immediately.<br>That team will notify all important authorities (police, insurance, etc).<br>List of things in the office: Financial reports, files, computers, possibly any laptops, supplies.<br>Once able to reenter, will assess what has been lost.<br>Now, due to CHOICE mainly using SharePoint, most things are saved online. |

| | |
|---|---|
| Logging into Wi-Fi, or plugging into the wall | There is a risk at the UN and when using public Wi-Fi or plugging a laptop into the wall, someone can hack into our computers and steal data.<br>Notify DPO immediately.<br>DPO calls with the person to discuss a recollection of how this happened, what was lost.<br>DPO informs Board member, and all have a call together to discuss next steps.<br>The DPO should work with the person who flagged the data breach to notify the relevant parties of what happened, what data (as exact as possible) has been breached, and what future steps will be taken.<br>Everyone in the organization will be required to change all of their passwords related to CHOICE.<br>If our data is leaked, we will need to write a comprehensive report about what sensitive information has been lost and the possible consequences. |
| Limited options to protect data | There are some cases where CHOICErs cannot fully secure their computers, accounts or data. When this happens, we have some steps CHOICErs should follow<br><br>Using Public Wi-Fi<br>We ask that CHOICErs use their judgement to assess as to when it is necessary. If CHOICE staff are travelling, and they suspect unsafe public Wi-Fi, then we encourage them to use a hotspot and reimburse the cost of the data.<br>If data does get leaked through public Wi-Fi, please follow steps above for, “Account hacked/data leaked”<br><br>Inability to use MFA<br>Sometimes CHOICErs cannot use MFA. We ask that CHOICErs do everything within their power to set it up. To turn it off, they must request from the OM. We ask that they create and use a very strong password in this case.<br>If data does get leaked due to no MFA, please follow steps above for, “Account hacked/data leaked” |

**Future Steps for CHOICE**

As CHOICE is a small organization with limited capacity, we have limited availability and funds to create a comprehensive GDPR, Privacy and Cyber Security Policy quickly. Rather than hiring a consultant to review our internal processes and policies CHOICE will use our collective knowledge and connections with expertise.

Below are some (prioritized) steps we will be taking/looking into to further advance our GDPR, Privacy and Cyber Security Policy and Processes:

| Action | Notes/Contacts | Timeline/Done |
|---|---|---|
| Board, Shelley and Timo review this document | We will have our Board review this document of policy and processes. We will also use our trusted knowledge expertise of 1. Timo on the advisory board, and 2. Shelley, Helena's mom who works in GDPR law | End of September |
| Contact The Trusted Third Party (TT3P) for a review of our policies and processes | Helena has been in contact with them. They previously offered their expertise to set everything up at a cost, but we do not have funds available for this. They also offered for them to review what we come up with.<br><br>Specifically ask them about working in non-EU countries.<br><br>Patrick Jordens: patrick.jordens@tt3p.nl | After Board reviews this document and CBF approves us |
| Risk and Gap Analysis | Create another overview of more things to include based on the CBF Requirements | October |
| Check and Audit Report | | November |
| Annual refresher for CHOICERs | | November GM, Nov 7th |
| Fake phishing email | Randomized every year to ensure the surprise factor | |
| Look into a VPN for those who travel often or to high-risk places | | |
| Look into applying MFA for the computers staff use | This would mean that every time a staff member opens their computer a multi-factor authentication would pop up. | |

| | | |
|---|---|---|
| | This would mean another MFA on top of the MFA we have for Microsoft 365. Might be costly | |
| Look into remotely disabling computers | Remote Desktop<br>Find and lock a Windows device<br>Citrix - open from another location | |