Last updated: March 2020

Data protection policy

March 2020

1. Background

Being based in the Netherlands, The Global Network of Young People Living with HIV (Y+) will apply a data protection policy that is in line with the Dutch data protection requirements.

The General Data Protection Regulation (GDPR or Algemene Verordening Gegevensbescherming (AVG) in Dutch) has replaced the Dutch Data Protection Act (Wet bescherming persoonsgegevens, Wbp). This new European privacy law tightens rules and regulations pertaining to the automatic processing of personal data. Under the GDPR, entrepreneurs are obliged to take extra measures when storing data on customers, staff and other persons.

The GDPR stipulates that suitable measures must be taken to protect data pertaining to customers and employees. Organizations may not, for example, collect and further utilize more personal data than absolutely necessary. They must also limit access to personal data.

The GDPR requests that organizations justify the registration and use of data in their possession. They must tell clients or employees which personal data they intend to use and what for. They must also provide own details (company name and address) and inform them if they intend to share personal data with other organizations. It is mandatory to include a privacy statement on their website.

2. Purpose

Y+ aims to process all personal data for which it is responsible in a safe and secure manner. The purpose of this data protection policy is to ensure that Y+'s standards and procedures around data protection are consistent with current data protection legislation and good practice guidance. The policy sets out the principles that we apply when processing the personal data of employees, supporters, service users, consultants, and anyone else whose data we process in the course of Y+ activities. The policy also sets out the responsibilities of staff in relation to the processing of personal data.

3. Scope

This policy applies to all Y+ staff and to consultants and contractors who undertake work on behalf of Y+. Y+ staff includes staff based at Y+ branch and subsidiary offices overseas.

4. Definitions

- *Personal data* means data relating to an individual who can be identified either from those data alone, or from the data in combination with other information. Personal data can be factual (e.g. name, email address, date of birth) or an opinion about a person's actions or behavior.

- *Special category data (sensitive data*) means personal data consisting of information regarding a person's: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life; the commission or alleged commission by them of any offence, or any proceedings in respect of any offence committed or alleged to have been committed.

- *Processing* means any activity that involves the use of personal data. Processing means carrying out any operation or set of operations on the data, including organizing, amending, disclosing, destroying, and transferring to third parties. Processing also includes obtaining,

recording and storing the data.

- *Data controller* means the person or organization that determines the purposes and means of processing personal data.

- *Data processor* means the person or organization responsible for processing personal data on behalf of a data controller.

5. Principles

Y+ follows the seven principles set out in Article 5 of the GDPR when processing personal data. These principles are:

1) **Lawfulness, fairness and transparency**
   Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

2) **Purpose limitation**
   Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

3) **Data minimization**
   Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4) **Accuracy**
   Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5) **Storage limitation**
   Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

6) **Integrity and confidentiality**
   Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

7) **Accountability**
   The data controller [in our case, Y+] shall be responsible for, and be able to demonstrate compliance with the six principles set out above.

6. Lawful basis for processing

Article 6 of the GDPR sets out the bases under which processing of personal data shall be lawful. Y+ must be clear about the legal basis that applies for any personal data that we process. The GDPR states that processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a **legal obligation** to which the controller is subject;
d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

While some processing at Y+ will be carried out on the basis of legal obligations (for example, the requirement for the organization to submit certain employee data to Dutch authorities for the purposes of statutory compliance) and the performance of contracts, the legal bases that will apply to most of our data processing operations are consent and legitimate interests.

Consent must be explicit (Y+ should be able to demonstrate that it has been given, whether through a written declaration or by electronic means such as a tick box on the Y+ website) and it must be specific (that is, for a single, clearly-defined purpose). The GDPR also requires that consent must be freely given; for example, consent cannot be freely given if the performance of a contract is conditional on consent being given for the processing of data not necessary for the performance of that contract.

Legitimate interests is the most flexible lawful basis for processing and is likely to be most appropriate where we use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. There are three elements to the legitimate interests basis. To rely upon this basis for processing an individual's data, we would need to (i) identify a legitimate interest; (ii) show that the processing is necessary to achieve it; and (iii) balance it against the individual's interests, rights and freedoms. All of this would need to be documented, in order that we can demonstrate compliance with the data protection principles set out in section 5 above.

7. Privacy notices

Either before or at the time of collection of any personal data by us, we are required to inform data subjects about what kind of personal data we collect, the reason for collecting the data, the purposes of the processing, the legal basis which we are relying on, the data subjects' rights in relation to that data, security measures taken in relation to data, whether we transfer data to third parties, the retention period and any potential transfers of data outside of the EU.

8. Individuals' rights

The GDPR provides the following rights for individuals. Y+ will honor these rights and comply with any requests made by data subjects in respect of these rights.

1. The right to be informed	The GDPR requires us to provide individuals with 'fair processing information' – this includes what we do with their personal data, the purpose of the processing and the lawful basis for the processing.
2. The right of access	Individuals have the right to access their personal data and supplementary information. The GDPR clarifies that the reason for allowing access is so that individuals are aware of and can verify the lawfulness of the processing.
3. The right to rectification	The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete.
4. The right to erasure	The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
5. The right to restrict processing	Individuals have a right to 'block' or suppress processing of personal data. In such cases, we are permitted to store the personal data but not further process it – we should retain just enough information about the individual to ensure that the restriction is respected in future.
6. The right to data portability	This right allows individuals to obtain and reuse their personal data for their own purposes across different services. An individual can ask us to provide copies of the personal data that we hold about them in a commonly-used and easily storable format.
7. The right to object	Individuals have the right to object to us processing their data, whether that processing is direct marketing (including profiling), processing for the purposes of scientific/historical research and statistics, or processing on the basis of legitimate interests.
8. Rights in relation to automated decision-making and profiling	The GDPR has provisions on: automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Y+ does not currently use automated decision-making and profiling in its activities.

9. Third party data processors

Where external companies are used to process personal data on behalf of Y+, responsibility for the security and appropriate use of that data remains with Y+.

Where a third-party data processor is used:

(a) a data processor must be chosen which provides sufficient guarantees about its data security measures to protect the processing of personal data;
(b) reasonable steps must be taken that such security measures are in place;
(c) the contract between Y+ and the third party must set out what personal data will be processed and the purpose of the data processing, and must require the third party to process data in accordance with the requirements of the GDPR.

If we are processing personal data jointly with an independent third party, the respective responsibilities of Y+ and the third party must be explicit in the agreement between the parties.

10. Transfer of personal data outside the EU

The GDPR restricts the transfer of data to countries outside the EU in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. A transfer of data to a different country takes place not only when data is sent or transmitted to that country but also if it can be viewed or accessed in that country.

Y+ will only transfer personal data outside the EU if one of the following conditions applies:

a) the European Commission has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms. The countries currently approved can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

b) the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

c) the transfer is necessary for one of the other reasons set out in the GDPR including:
    i) the performance of a contract (e.g. Y+ staff based overseas and employed by a PEO (professional employer organization)),
    ii) to establish, exercise or defend legal claims or
    iii) to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent.

Before transferring personal data outside of the EU, staff must check with the Y+ chief executive whether or not the proposed transfer meets relevant requirements.

11. Children

Where collection of personal data relates to a child under the age of 18, and we are relying on consent to process that data, we must ensure that parental or guardian consent is given, in writing, prior to the collection.

Due to the sensitive nature of the matter, Y+ does not collect visual documentation of children under 18 years old, including photos, videos or audio documentation.

12. Special category data (sensitive data)

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. In order to lawfully process special category data, we must identify both a lawful basis for processing (see Section 6 above) and a separate condition for processing special category data as required by Article 9 of the GDPR.

Special category data includes information about an individual's race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation. (It does not include personal data relating to criminal offences and convictions; there are specific safeguards for this type of data elsewhere in the GDPR.)

The nature of Y+'s work means that it often requests special category data from individuals, whether during program implementation or as part of its monitoring and evaluation processes.

Y+ will only process special category data under strict conditions, including:

- where the individual has given explicit consent to the processing of their personal data;
- where the law requires us to process the data for employment purposes;
- where the processing is necessary to protect the vital interests of the individual.

13. Data breaches

The GDPR requires that we report to the Information Commissioner's Office (ICO), within 72 hours of first becoming aware, any personal data breach where there is a risk to the rights and freedoms of the data subject (the individual whose personal data is affected). There is also a requirement to report certain personal data breaches to the data subjects themselves.

Y+ has put in place procedures to deal with any suspected personal data breach and will notify data subjects or the ICO where we are legally required to do so.

If anyone at Y+ knows or suspects that a personal data breach has occurred, they should immediately contact the Y+ Director of Programmes, Management and Governance. They must retain all evidence relating to personal data breaches to enable Y+ to maintain a record of such breaches, as required by the GDPR.

14. Data retention policy

In order to ensure that personal data held by Y+ is not kept for longer than necessary, the Data Retention Policy (Appendix A to this Data Protection Policy) sets out how Y+ will meet the requirements of current legislation and follow best practice in this area.

The Data Retention Policy applies to organizational data as well as personal data and relates to data

held internally within the organization and also externally with third party suppliers. The policy covers all documents and records of whatever sort, whether hand-written or printed, hard-copy or electronic. 'Documents and records' includes (but is not limited to) letters, reports, e-mails, invoices, bank statements, contracts, agreements, annual returns and minutes of meetings.

15. Responsibilities

Y+ is the data controller of all personal data relating to it and processed in the carrying out of its activities. The Y+ Board of Trustees is ultimately responsible for the establishment of policies and procedures to ensure compliance with applicable data protection law.

The organizational lead on data protection is the Y+ Director of Programmes, Management and Governance of Y+ who is responsible for ensuring maintenance and implementation of this policy, advising on data protection issues, liaising with the ICO, and supporting staff responsible for data processing in specific clusters or subject areas (e.g. HR, monitoring and evaluation, communications) to develop and maintain appropriate data protection procedures.

Individual responsibilities
Y+ staff, consultants and contractors may have access to the personal data of other individuals in the course of their employment or during the fulfilment of a contract. Where this is the case, Y+ relies on them to help meet its data protection obligations.

Staff, consultants and contractors who have access to personal data are required:

- To access only data that they have authority to access and only for authorized purposes;
- Not to disclose data except to individuals (whether inside or outside the organization) who have appropriate authorization;
- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- Not to remove personal data, or devices containing or that can be used to access personal data, from the organization's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- Not to store personal data on local drives or on personal devices that are used for work purposes; and
- To report data breaches of which they become aware to the Y+ data protection officer immediately.

Failure to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Y+ disciplinary policy. Significant or deliberate breaches of this policy, such as accessing Y+ employee records or other personal data without authorization or a legitimate reason to do so, may constitute gross misconduct.

16. Training and support

Y+ will ensure that all Y+ staff undergo adequate training to enable them to comply with data protection law. Y+ will also regularly test its systems and processes to assess compliance.

All new staff are required to undergo data protection training as part of their induction procedure. Data protection update sessions are presented on an ad hoc basis during monthly staff meetings, and dedicated data protection training sessions for all staff are held on a regular basis.

Additional training and support can be provided to individuals and teams as required.

Appendix A - Data Retention Policy

Document retention tables

Income and banking documentation		
Document	**Retention period**	**Reason for retention period**
Bank statements	Seven years	Netherlands Tax Regulations
Correspondence re donations		
Bank reconciliations		
Receipts cash book		
Bank ledgers		
Payment requests		
Grant agreements	Seven years – unless donors require longer period	Netherlands Tax Regulations + donor regulations
Legacies	Seven years	Netherlands Tax Regulations

Purchase invoices and supplier documentation		
Document	**Retention period**	**Reason for retention period**
Payments cash book or record of payments made	Seven years	Netherlands Tax Regulations
Purchase ledger		
Invoices		
Petty cash records		

Payroll documentation		
Document	**Retention period**	**Reason for retention period**
Payroll and payroll control account	Seven years	Netherlands Tax regulations
Notice to employer of tax premiums		
Annual return of employees and directors expenses and benefits		
Records of pension deductions Deeds of covenant/ Gift Aid		

Employee/Personnel records		
Document	**Retention period**	**Reason for retention period**
Details of medical schemes	Permanently	Commercial
Organisation charts	Permanently	Commercial
Staff personnel charts	Five years after employment ceases	Commercial
Wages and salary records	Seven years plus the current year	Netherlands Tax Regulations
Expense accounts/records		
Redundancy details, calculations of payments, refunds	Seven years after employment has ceased	Netherlands Tax Regulations
Notifications to the Immigration	Five years after employment has ceased	Internal regulations

Applications for jobs - where the candidate is unsuccessful	Four weeks after notifying the unsuccessful candidate	Data Protection Act
Statutory Maternity Pay records, calculations or other medical evidence	Seven years	Netherlands Tax Regulations
Sickness records	Three years after the end of each tax year for Statutory Sick Pay purposes	Internal regulations

Insurance documents		
Document	**Retention period**	**Reason for retention period**
Policies	Seven years	Internal regulations
Claims correspondence	Seven years	Internal regulations
Accident reports and relevant correspondence	Seven years	Internal regulations

Other documents		
Document	**Retention period**	**Reason for retention period**
Trustee/director minutes or meetings and decisions	Permanently	Internal control
Annual accounts and annual review	Permanently	
Major agreements of historical significance	Permanently	
Fixed assets register	Permanently	Netherlands Tax Regulations
Contracts and agreements of all kinds, including contracts with suppliers, licensing agreements, rental/ hire purchase agreements, indemnities and guarantees, and other agreements or contracts.	Seven years	Netherlands Tax Regulations Donor Regulations
Records of major refurbishments, warranties, planning consents, design documents, final health and safety files.	Seven years	Netherlands Tax Regulations