Privacy Policy

Using this site

By using and/or visiting the CYBER POLICY CENTRE website you signify your agreement to the terms and conditions which follow.

CYBER POLICY CENTRE may modify or revise these terms and conditions and any related policies at any time, and you agree to be bound by such modifications or revisions.

Using information on cyberpolicycentre.org

CYBER POLICY CENTRE aims to ensure that the content and information provided here is accurate at the time of posting, however we we cannot guarantee the absolute accuracy information contained in its pages all the time, and any person using information contained in them does so entirely at their own risk.

Copyright

Protecting your privacy

CYBER POLICY CENTRE is committed to protecting your privacy. We only collect data from you when you register to receive updates from us. We will use user data we collect from you only in accordance with the following guidelines:

- to provide updates to you
- to provide and improve our service to you, to notify you of any changes to our terms and conditions of us
- collection of personal data is subject to our Data Protection Policy.

The CYBER POLICY CENTRE regards the lawful and correct treatment of personal information as crucial to upholding our values and to maintaining confidence between us and those with whom we carry out our work. We ensure that we treat personal information lawfully and correctly.

The CYBER POLICY CENTRE Data Security Policy outlines our undertakings with regard to compliance with data protection law and is designed to support:

- Compliance with data protection law and good practice
- Protection of privacy rights of supporters, beneficiaries, partners and staff
- Openness about how we handle confidential and personal data
- Management of risk
- Standards of good practice in accordance with our publicly stated principles.

Links to third party websites

Within this website we include links to third party advice that may be of use to our users. When using the site, you may gain access to other websites through use of links or hypertext. In using this site you agree that CYBER POLICY CENTRE is not responsible for the advice given by the third party organisations or for the content or operation of such third party websites.

CYBER POLICY CENTRE, to the extent permissible by law, excludes all liability which may arise from your use or reliance on the information or contents contained in the linked site.

About Cookies

A cookie is a file containing an identifier a string of letters and numbers that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.

Cookies may be either ‘persistent’ cookies or ‘session’ cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed. Cookies do not typically contain any information that personally identifies a user, but personal information that we store about you may be linked to the information stored in and obtained from cookies.

Cookies can be used by web servers to identify and track users as they navigate different pages on a website and identify users returning to a website.

How ARTICLE 19 uses cookies

CYBER POLICY CENTRE uses cookies on its website to understand more about users and to improve their experience across the website. The purposes for which they are used are set out below:

- to improve the website’s usability
- to analyse the use of the website
- to administer the website
- to improve the security of the website

We use Google Analytics Universal to analyse the use of our website. Our analytics service provider generates statistical and other information about website use by means of cookies.

The information generated relating to our website is used to create reports about the use of our website. Our analytics service provider's privacy policy is available at here.

Managing your cookie settings

Most browsers allow you to changing your settings and preferences for cookies. Use the links below to take a look at individual browser settings:

- Internet Explorer – our website only supports IE11 or above
- Chrome
- Firefox
- Safari
- Safari (IOS)
- Blackberry
- Windows phone

If you are using a browser we have not included above please refer to their website and support services.

Data Protection Policy

1. Context

1.1. Introduction

CYBER POLICY CENTRE may have to collect and use information about people with whom we work, as well as people who have expressed an interest in the work we do.

The CYBER POLICY CENTRE regards the lawful and correct treatment of personal information as crucial to upholding our values and to maintaining confidence between us and those with whom we carry out our work. We ensure that we treat personal information lawfully and correctly.

The CYBER POLICY CENTRE Data Security Policy outlines our undertakings with regard to compliance with data protection law and is designed to support:

- Compliance with data protection law and good practice
- Protection of privacy rights of supporters, beneficiaries, partners and staff • Openness about how we handle confidential and personal data
- Management of risk • Standards of good practice in accordance with our publicly stated principles

1.2 Objectives

This policy seeks to:

1. Protect the rights of individuals by ensuring that all personal data held by us is used appropriately and lawfully
2. Ensure that all collection, processing, storage and sharing of personal data by CYBER POLICY CENTRE complies with data protection principles and legal requirements
3. Maintain the confidence of data subjects in CYBER POLICY CENTRE
4. Ensure the organisation meets the requirements of the General Data Protection Regulation (GDPR) and national data protection legislations
5. Inform and enable employees, job applicants, suppliers and contractors.

1.3 Application

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our work. It also covers our response to any data breach and other rights under the GDPR and national legislations.

Application of this policy applies to:

- All employees, freelancers and contractors of CYBER POLICY CENTRE
- Any donors, partner organisations or representatives who are privy to information held by CYBER POLICY CENTRE and protected under the GDPR , DPA and data protection legislations The policy applies to the personal data of people with whom we work, job applicants, existing and former employees, fellows, directors, and self-employed contractors, and supporters.

These are referred to in this policy as relevant individuals.

1.4 Definitions

CYBER POLICY CENTRE collects processes and stores certain types of personal data. "**Personal data**" is any information that enables another person to directly or indirectly identify a person from that information: for example, a person's name, address, email, identification number, location. It can also include pseudonymous data. CYBER POLICY CENTRE will hold this category of personal data for the purposes of communication and management within the limits of appropriate and lawful use, and subject to our Acceptable Use Policy.

Other "**special categories of personal information**" include data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

CYBER POLICY CENTRE may from time to time undertake due diligence process that may involve viewing "**Criminal offence data**": this is data which relates to an individual's criminal convictions and offences. However, this information will only be held, if at all, for the duration in which lawful processing takes place, such as recruitments, due diligence investigations for partnerships, appointment of Trustees and related matters of financial management.

1.5 Data Protection Law

The global regulations which are in force through GDPR and data protection legislations purpose it to protect information held about people both in manual records, on computers, platforms and devices, and to enforce a particular set of standards for the processing of that information.

Under GDPR and national data protection laws, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

1. processing will be fair, lawful and transparent
2. data be collected for specific, explicit, and legitimate purposes
3. data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
4. data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
5. data is not kept for longer than is necessary for its given purpose

6. data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
7. we will comply with the relevant GDPR procedures for international transferring of personal data In addition the new General data protection regulation (GDPR) seeks clarity on how permission to hold data was obtained, and how the data is maintained.

The following principles apply to the CYBER POLICY CENTRE Data Protection Policy as follows:

Principle 1 The organisation uses data for the express purpose it was collected from the data subject; that the purpose for the collection was consented to by the data subject; and that the data subject is informed as to their right to opt out rather than opt in for any additional use of data.

Principle 2 Where data has been obtained from third parties, the organisation processes data for the purpose that it has been collected by the third party; and that the data subjects have consented to the use to which data has been processed (whether by CYBER POLICY CENTRE or the third party); and that in consenting the data subject opts in to the use of data.

Principle 3 The organisation creates and maintains adequate records identifying the data held, where it came from and who we share it with. Note – "Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2. Data and Security

2.1 Types of data held by us

CYBER POLICY CENTRE retains three broad categories of data which enable us to operate. The three categories are:

- Marketing and fundraising data
- Grant implementation, project and organisational financial data
- Prospective, current and past employee data

Aligned with principles of lawful use, CYBER POLICY CENTRE collects and processes data gathered from individuals who have opted into our marketing and communications channels. We hold information as follows:

Marketing and fundraising data**:** a) Name, postal addresses, phone number; b) email addresses; c) job title and organisation; d) details of donations made by the data subject or, more usually, the organisation which they work for

Grant implementation and organisational financial data: In addition to personal information as above, during the creation and implementation of grants, and operations the following financial data is processed by CYBER POLICY CENTRE: a) tax codes and bank account details; b) insurance details and details of next of kin.

Recruitment process and employee data: We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We hold this data within our enterprise information systems and we also keep this data in a personnel file relating to each employee within our computer systems. Specifically, we hold the following types of data for employees:

1. personal details such as name, address, phone numbers, passport details;
2. information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education and employment history etc;
3. details relating to pay administration such as National Insurance numbers, bank account details and tax codes;
4. pension and insurance details (eg: next of kin);
5. medical or health information;
6. information relating to your employment with us, including: job title and job descriptions, salary, terms and conditions of employment, formal and informal proceedings such as letters of concern, disciplinary and grievance proceedings, annual leave records, appraisal and performance information, internal and external training modules undertaken; expenses paid during travel or other circumstances; benefits claimed including gym membership and dental insurance.

All of the above information is required for our processing activities. More information on processing activities are included in our privacy notice for employees.

2.2 Your rights under this policy

You have the following rights in relation to the personal data we hold on you:

i. the right to be informed about the data we hold on you and what we do with it;

ii. the right of access to the data we hold on you. More information on this can be found in the section headed “Access to Data” below and in our separate policy on Subject Access Requests”;

iii. the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected.

iv. the right to have data deleted in certain circumstances.

v. the right to restrict the processing of the data;

vi. the right to transfer the data we hold on you to another party.

vii. the right to object to the inclusion of any information;

viii. the right to regulate any automated decision-making and profiling of personal data.

(*Note for employees:* more information can be found on each of these rights in our separate policy on employee rights under GDPR.)

2.3. Our Responsibilities

In order to protect the personal data of individuals, we have ensured that those responsible for processing data inside CYBER POLICY CENTRE, are aware of our policies on data protection.

i. Where it is necessary for CYBER POLICY CENTRE to pass personal data to third parties for processing, we always seek assurance from the third party that it will abide by the requirements of the GDPR na dother relevant national legislations on data protection. For long-term suppliers we will always sign third party data protection agreements before sharing our data. Short-term suppliers will always sign a service agreement by which they are required to abide by our Data Protection Policy.

ii. We will always ensure that we have consent to share this information and that we use the data appropriately and lawfully

iii. We have also appointed employees with responsibility for reviewing and auditing our data protection systems. Each individual that handles sensitive, personal or confidential data will be nominated and named within the organisation and have clear responsibility for the processes and management of that data.

iv. Responsibilities for CYBER POLICY CENTRE data processes will include ensuring that the data is either retained, updated or destroyed in line with these policies.

v. CYBER POLICY CENTRE 19 maintains clear retention periods and rules for updating or deleting all personal information once it is no longer required

2.4: Lawful basis for processing

We ensure that processing is only carried out where a lawful basis for processing exists, and in addition, where we have assigned a lawful basis against each processing activity. Where no other lawful basis applies, we may seek to rely on the individual's consent in order to process data. However, we understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate.

Employees will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

2.5 Access to data

As stated above, individuals have a right to access the personal data that we hold on them. To exercise this right, individuals may make a **Subject Access Request.** We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, further information will be required and a reasonable charge will be applied. Further information on making a subject access request is contained in our Subject Access Request policy.

2.6 Data Disclosures

CYBER POLICY CENTRE will never share data outside of the organisation without prior consent, except in the following circumstances primarily related to human resources management. Circumstances leading to such disclosures include, but are not exclusive to:

a) employee benefits operated by third parties, such as pension information, health and insurance; b) disabled individuals – where reasonable adjustments involving a third party, are required to assist them at work; c) individuals' health data – to comply with health and safety or occupational health obligations towards the employee; d) for Statutory Sick Pay purposes; e) HR management and administration – to consider how an individual's health affects his or her ability to do their job; f) the smooth operation of any employee insurance policies or pension plans; g) to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty h) provision of information to our statutory auditors and project auditors where required by donors..

These kinds of disclosures will only be made lawfully, and when strictly necessary for the purpose.

2.6 How we maintain data security

CYBER POLICY CENTRE operates with a high degree of awareness of risks associated with data privacy and security. As such we maintain a number of secure enterprise systems that support the work of finance, human resources, project management and communications and fundraising teams.

Personal information and relevant data are retained within these systems, and all processing activities are subject to our **Acceptable Use Policy.** In summary data processors in CYBER POLICY CENTRE are required to implement the following practices:

A. Collecting Data

1. Individuals are asked for their consent before CYBER POLICY CENTRE collects or stores their data.

2. Individuals are made clearly aware of the purpose for which their data has been collected, will be used, disclosed, retained and disposed of.
3. Individuals are given an option to ‘opt in’ to receive follow up and marketing information and the “opt-in” must follow best practice guidelines. Consent will not be inferred if an individual does not respond to a consent request.
4. Individuals will be informed of their right to complain to the relevant office if CYBER POLICY CENTRE is found in breach of data protection rules.
5. CYBER POLICY CENTRE employees, will only use data for the purposes for which permission have been given.
6. We ensure that consent is appropriate for the age and capacity of the individual and to the particular circumstance. (Specific rules apply for individuals who may be children or vulnerable adults.)
7. If there is a need to collect children’s data CYBER POLICY CENTRE will verify peoples ages and gather parental or guardian consent for anyone under 18 years of age.

B. Storing Data

1. Data collected by CYBER POLICY CENTRE is stored securely in our enterprise information systems.
2. No data is stored on platforms such as Google Docs. (Google stores and backs up its data in the US, which is contrary to data protection law.)
3. Data is downloaded from our systems and processed on excel sheets, prior to either: a. reloading into the systems. b. Producing a mailing list for which consent has been provided.
4. Under no circumstances is personal data retained on spreadsheets once the purpose of doing so has been completed.
5. Personal data stored on hard drives on various document formats (MS Office suite; Apple formats; Adobe PDFs etc) should be deleted and shredded, once the purpose has been fulfilled.
6. Under no circumstances should personal data be downloaded onto USB devices, or distributed by mobile devices for use outside CYBER POLICY CENTRE and its affiliates.

C. Sharing Data

1. In all cases, individuals will be asked for consent to share information across CYBER POLICY CENTRE entities, and where necessary, third parties.
2. Individuals will always be given an option to ‘opt in’ for use of their data for other means
3. And in all cases, consent will be appropriate for the age and capacity of the individual and to the particular circumstance
4. Before sharing any data externally, approval is obtained from the Executive Director. Data that is shared after approval is encrypted.
5. Before approving the sharing of data, a third party data sharing agreement has to be in place within the organization.
6. Data that is confidential, sensitive, or poses an explicit security risk is never shared by anyone other than a senior manager and only with the approval of the Executive Director.

7. A record of all instances where data has been shared with third parties is maintained. The list identifies the purposes for which it is shared, the security measures undertaken and the nature of the consent by the individual.
8. Sensitive data might include:

    - Passport information shared with transport agencies an hotels
    - Budgetary information (including employees' salaries)
    - Personal contact details (email addresses, phone numbers)
    - Personal information about an individual who we are working with
    - Confidential details about a project

D. Removing Data

1. When removing data stored on electronic files, the information will be permanently removed from the device.
2. Paper documentation with sensitive information, such as recruitment documentation will be destroyed using a cross-cut shredder or a service that guarantees safe removal and disposal for any paper files that no longer is need.
3. Staff do not under any circumstances leave personal data attributable to individuals, on their desk.

3. Third Party Processing and International Data Transfers

3.1 Third Parties

Where we engage third parties to process data on our behalf, we use a data processing agreement with the third party to ensure that your data meets the requirements of GDPR and other relevant laws and that your data is protected to at least the same standards, once it is transferred.

As noted above, the range of third parties includes those relevant to employees, such as payroll and pension providers. However, for all individuals we will never share your data with any third party without your consent.

3.2 International Data Transfers

CYBER POLICY CENTRE may be required to transfer personal data to its Affiliates in country or countries outside of Africa. Transfers may take place because it relates to a CYBER POLICY CENTRE activity, such as a campaign, or to the announcement of new resources or events. Where this occurs, safeguards are adopted as detailed in clause 2.6 above.

3.3 Data Processing Risks

Throughout CYBER POLICY CENTRE many individuals collect, store and use different types of data, including contact details, personal information and sensitive budgetary information. When we lawfully share this information internally and externally with other organisations it is vital that all (internal or external) parties involved recognise the risks of handling potentially sensitive data, and comply with the policies that seek to protect the organisation and individuals.

That is why we have agreements in place that require us to protect information when share certain types of information between ourselves and third parties. In doing so we seek to avoid risks associated with :

- Breaches of confidentiality eg: information shared inappropriately and without permission
- Endangerment to individuals: where an individual's safety and security has been placed at risk
- Reputational damage: eg: companies and individuals could be subject to complaints if data is obtained, stored, managed and shared inappropriately
- Enforcement Action; for serious breaches and non-compliance with data protection rules, severe fines and penalties such as information audits may result in serious risk to the functioning of the organisation.

3.4 Notification of data breach

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the relevant authority within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

(*Note: A data breach relates to the loss of personal data and should be notified following the procedure described. A security breach relates to the loss of equipment containing personal data.)*

Where a security breach has been notified that also involves personal data, we follow the data breach policy. Examples of a breach include:

- personal data accidentally being sent to someone (either internally or externally) who does not have a legitimate need to see it;
- databases containing personal data being compromised
- loss or theft of laptops, mobile devices, or paper records containing personal data;
- paper records containing personal data being left unprotected for anyone to see, for example:- — files left out when the owner is away from their desk and at the end of the day; — papers not properly disposed of in secure disposal bins that can then be extracted or seen by others; — papers left at photocopying machines;
- employees accessing or disclosing personal data outside the requirements or authorization of their job;
- being deceived by a third party into improperly releasing the personal data of another person; and
- the loss of personal data due to unforeseen circumstances such as a fire or flood.

More information on breach notification is available in our Breach Notification policy.

4. Data Protection Roles

4.1 ARTICLE 19 data protection roles

In the context of GDPR the entities described as CYBER POLICY CENTRE constitute the role of **Data Controller** even though CYBER POLICY CENTRE operates outside of the EU, the organization complies with the standards of data protection in our polices, and the GDPR.

Data Protection Officer: The GDPR requires organizations of a certain type and size to have a dedicated Data Protection Officer (DPO). It is broadly accepted that CYBER POLICY CENTRE falls into the category of organisation where the responsibilities of the DPO are handled through the directorship. These responsibilities include: i) Ensuring that there is a data policy in place, that it is up to date, monitored and actioned; ii) Assessing if any incidents involving data breaches are required to be communicated to the information commissioner and data subjects; iii) Advising the wider organisation on data use, what we can do with it and how we are allowed to use it; iv) Ensuring CYBER POLICY CENTRE terms and conditions are correct and up to date and that information is maintained in accordance with the terms and conditions; v). Assessing the risk of reputational damage of any data breach; vi) Communicating to the wider organization any data changes and updates that should be known to them; vii) Conducting a regular data audit to ensure that existing data is being used and maintained appropriately; viii) Advising on the appropriate timeframe data can be used for, conducting a regular review of the use of existing data and advising on what should be destroyed.

Data Processor: This role is assumed by a minority of CYBER POLICY CENTRE employees who are responsible for processing data through our enterprise systems. All employees in these roles have been identified and undergo training on data protection and security.

All new employees must read and understand the policies on data protection as part of their induction, and receive training, covering information about confidentiality, data protection and the actions to take upon identifying a potential data breach. All employees who need to use our enterprise systems are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the organisational of any potential lapses and breaches of the CYBER POLICY CENTRE's policies and procedures. In practice all employees are expected to abide by the Acceptable Use Policy.

5. Retention and Record Keeping

5.1 Statutory retention periods

CYBER POLICY CENTRE retains personal information for the formal statutory periods to facilitate several organisation wide functions, such as human resources management, financial management and governance.

CYBER PLOCY CENTRE Retention Periods

Statutory

- Retirement Benefits Schemes: – 6 years from the end of the scheme year
- Statutory Maternity Pay (calculations, certificates, medical evidence) – 3 years after the end on the tax year in which the period ends
- Wage/salary (overtime, bonuses, expenses) – 6 years
- National Minimum Wage – 3 years after the end of the consequent pay reference period
- Working hours – 2 years after they are made

Recommended

- Application forms and interview notes – 6 months to a year
- Assessments under health and safety regulations and records of consultations with safety representatives and committees – permanently
- Money purchase details – 6 years after transfer or value taken
- Pension scheme investment policies – 12 years from the ending of any benefit payable under the policy
- Pensioners' records – 12 years after end of benefit
- Personnel files, training records (disciplinary records, working time records) – 6 years after end of employment
- Redundancy details, calculations of payments, refunds, notification to the Secretary of State – 6 years after date of redundancy

5.2 Record keeping

CYBER POLICY CENTRE keeps records of its processing activities including the purpose for the processing and retention, in the form of a data asset record. Each record includes: i). the name and contact details of the controller and the data protection officer; ii). the purposes of the processing; iii). a description of the categories of data subjects and of the categories of personal data; iv). the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; v). where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation the documentation of suitable safeguards; vi). where possible, the envisaged time limits for erasure of the different categories of data; vii). where possible, a general description of the technical and organisational security measures in place.

Each data processor maintains a record of all categories of processing activities carried out on behalf of CYBER POLICY CENTRE, containing: i). the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; ii).the categories of processing carried out on behalf of each controller; iii). where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and documentation of suitable safeguards; iv). where possible, a general description of the technical and organisational security measures.

The records are maintained in writing, including in electronic form. CYBER POLICY CENTRE shall make the record available to the supervisory authority on request.

Although these obligations do not apply to an enterprise of the size of CYBER POLICY CENTRE because any data breach has the potential to result in a risk to the rights and freedoms of data subjects, we consider the record keeping an essential part of our data protection policy.