Name of policy	Data protection policy
Last updated	20th June 2019
Update interval	Every 3 years
Authorised sign-off	Board of Trustees

Cyan International Data Protection Policy

POLICY STATEMENT

1.1 We (Cyan International) are committed to protecting personal data and respecting the rights of individuals whose personal data we collect and use. In line with best practice we will seek registration as a data controller with the Information Commissioner's Office (ICO) .

We process personal data to enable us to, among other purposes:

1. Administer supporter records;

2. Fundraise and promote the interests of the charity;

3. Manage our representatives;

4. Maintain our own accounts and records;

1.2 Everyone has rights regarding the way in which their personal data is handled. In line with our values and aims, we are committed to good practice in the handling of personal and confidential information and to ensuring that such information is stored securely and is processed in accordance with the law.

2. PURPOSE OF THIS POLICY

2.1 This policy is designed to comply with relevant legislation including the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).

2.2 In the course of our work, we may collect and process personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, contractors who provide us with technical services or payment services).

2.3 We process the personal information of individuals in both electronic and paper form with all data protected under data protection law. In some cases, this will include sensitive information about individuals' religious or other beliefs, finances and personal circumstances. We also hold less sensitive information such as names and contact details, education and employment details, and visual images of current, past and prospective staff, mission personnel, volunteers, supporters, and contact details of advisers, complainants, enquirers, representatives of other organisations as well as business and other contacts such as suppliers. We may also receive other personal information from the above or other sources.

We are aware that individuals can be harmed if their personal information is misused, is inaccurate, if it gets into the wrong hands as a result of poor security or if it is disclosed carelessly.

2.5 We are committed to protecting personal data and information from unauthorised disclosure and ensuring its accuracy. Breaches of data security or confidentiality are serious incidents. If they occur, they will be investigated fully and actively managed to ensure that any breach is as limited as possible. We may also be required to report breaches to the Information Commissioner's Office (ICO) if a breach results in a risk to an individual, and to inform the data subject if the breach results in a high risk to any person.

3. DATA PROTECTION PRINCIPLES

3.1 Cyan International and contracted processors will comply with the GDPR's Principles. These provide that personal data must:

1. be processed lawfully, fairly and in a transparent manner (see section 8 below);

2. be processed for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes;

3. be adequate, relevant and limited to what is necessary for the purpose;

4. be accurate and, where necessary, up to date;

5. not kept longer than necessary for the purpose, unless it is retained for public interest, scientific, historical research or statistical purposes and appropriate measures are taken to safeguard the rights of data subjects;

6. be processed in a manner which ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational means

7. be processed in accordance with the rights of data subjects (see section 12 and Schedule 1)

8. not be transferred (or stored) outside the European Union (EU) unless this is permitted by the GDPR (see section 17). This includes storage on a cloud the servers of which are located outside the EU

4. FAIR AND LAWFUL PROCESSING

4.1 Fairness of processing means that we will only process data in the manner in which data subjects reasonably expect. In order to make data subjects aware of how we process personal data, the GDPR requires that we provide data subjects with certain information when we collect information from them as well as when we collect information about them from other sources.

4.2 If personal data is collected directly from data subjects, we will inform them (in writing) of the nature of the data collected and the relevant privacy notice.

4.3 If data is collected from a third party rather than directly from the data subjects, we will provide to the data subjects (in writing), within a reasonable time and not later than one month after we collect

the data, with the Cyan International Privacy Notice (appendix 1) and the nature of the data collected including:

1. The categories of data concerned;

2. The source of the personal data

If we use personal data collected in this manner for communicating with data subjects Cyan International will provide this information not later than the time of our first communication with them, and if we intend on disclosing any of the personal data we must provide this information before the disclosure.

If we collect data from the data subject and we are aware that we will later be collecting additional data from third party sources, it may be more effective to provide all the information to the data subject when we collect the data from them.

LAWFUL PROCESSING

4.4 Processing of data is only lawful if at least one of the conditions listed in Article 6 of the GDPR is satisfied. The main conditions on which we rely are:

1. Consent: the individual has given clear consent for you to process their personal data for a specific purpose

2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

3. Legal obligation: the processing is necessary for you to comply with the law

4. Vital interests: the processing is necessary to protect someone's life.

5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

6. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. When we rely on the legitimate interests ground we will carry out a balancing exercise, weighing our legitimate interests with the rights of the individuals concerned

4.5 When sensitive personal data is processed, we will satisfy one of the conditions set out in Article 9 of the GDPR. These include:

1. The data subject has explicitly given consent;

2. The processing is necessary for carrying out our obligations under employment and social security and social protection law;

3. The processing is necessary for safeguarding the vital interests (in life or death situations) of an individual and the data subject is incapable of giving consent;

4. The processing is carried out in the course of our legitimate activities and only relates to our members or persons we are in regular contact with in connection with our purposes;

5. The processing is necessary for pursuing legal claims. The GDPR provides other alternatives for processing sensitive personal data as well and before deciding on which condition should be relied upon, the original text of the GDPR should be consulted together with any relevant guidance.

4.6 Other than in the specific circumstances described in section 4.7, information relating to criminal convictions and offences will not be processed unless the processing is authorized by law or is carried out under the control of official authority. This includes information about (i) allegations of criminal offences' (ii) proceedings in relation to criminal or alleged offences; and (iii) the disposal of criminal proceedings including sentencing. Sensitive personal data can only be processed under strict conditions, including the data subject's explicit consent (although other alternative conditions can apply in limited, very specific circumstances as described below).

4.7 Sensitive personal data may be processed for the purpose of safeguarding children or individuals at risk where it meets the substantial public interest condition under Schedule 1, Part 2 of the Data Protection Act 2018 and the processing is necessary for:

1. protecting an individual from neglect or physical, mental or emotional harm; or

2. protecting the physical, mental or emotional well-being of an individual where that individual is aged under 18 or aged 18 and over and at risk and if the circumstances so demand, may be without the explicit consent of the data subject where obtaining consent would prejudice the provision of protection for the child or individual at risk.

5. CONSENT

5.1 If consent is the basis of justifying processing it can be withdrawn at any time and if withdrawn, the processing will cease. Data subjects will be informed of their right to withdraw consent.

5.2 The GDPR requires consent to be a freely given, specific, informed and unambiguous indication of the data subject's wishes. It must be a statement or clear affirmative action which signifies agreement to the processing of personal data relating to the member. As a result, presumed consent and pre-selected opt-in boxes will not constitute valid consent under the GDPR.

6. PROCESSING FOR SPECIFIED PURPOSES

6.1 We will only process personal data for the specific purposes set out in our Privacy Notice or for other purposes specifically permitted by law. We will notify those purposes to the data subject in the manner described in section 4 unless there are lawful reasons for not doing so and this is permitted by a legal exemption.

6.2 We may process data for further purposes which we might not have envisaged when providing the data subject with the original privacy notice as long as the further purpose is compatible with the

original purpose for which the data was collected. When assessing compatibility, we will consider, among all other relevant issues, the link between the purposes, the context in which the data was collected, the reasonable expectation of the data subject concerned, the nature of the personal data, the consequences of the further processing and the existence of appropriate safeguards. We are required to inform data subjects of the further purposes and provide them with appropriate additional information before we commence the further processing.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

7.1 We will only collect and use personal data to the extent that it is required for the specific purpose described in section 6 (which would normally be notified to the data subject). We should collect and use just enough information, which is relevant, to achieve that purpose, but not more than is required.

7.2 We will check records regularly for missing information and to reduce the risk of irrelevant or excessive information being collected.

7.3 When implementing systems which involve processing personal data we will consider how such systems can provide for data minimisation by design and by default as described in section 18.

8. ACCURATE DATA

8.1 We will ensure that personal data held is accurate and kept up to date within an appropriate timescale.

9. DATA RETENTION AND DESTRUCTION

9.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected, and we will comply with relevant guidance issued to our sector with regard to retention periods for specific items of personal data. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

9.2 Information about how long we will keep records for can be found in our Data Retention Schedule.

10. PROCESSING IN ACCORDANCE WITH DATA SUBJECTS' RIGHTS

10.1 We will process all personal data in line with data subjects' rights, in particular their right to:

1. Request access to any personal data held about them by us (the right of subject access is discussed in section 12 below),

2. Prevent the processing of their personal data for direct-marketing purposes (discussed in section 11 below);

3. Ask to have inaccurate personal data amended; and

4. Object to processing, in certain circumstances

11. DIRECT MARKETING

11.1 'Direct marketing' means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. This includes contact made by organisations to individuals solely for the purposes of promoting their aims and the advertising need not be of a commercial product, nor need anything be offered for sale. Cyan International will adhere to the rules set out in the GDPR, the Privacy and Electronic Communications Regulations and any laws which may amend or replace the rules governing direct marketing when we make contact with data subjects, whether that contact is made by (but not limited to) post, email, text message, social media messaging, telephone (both live and recorded calls) and fax. Stricter rules apply to marketing by email and other electronic means including text messaging, social media messaging, fax and automated telephone calls.

11.2 Any direct marketing material that we send will identify us as the sender and will describe how an individual can object to receiving similar communications in the future.
11.3 Data subjects have a very strong right to object to any form of processing of their personal data for a direct marketing purpose. If an individual exercises their right to object we will cease processing for this purpose within a reasonable time.

12. SUBJECT ACCESS REQUESTS (SARs)

12.1 All data subjects have a right to obtain from us copies of personal data which we hold about them. Schedule 1 sets out the information that will be provided along with the methodology by which a request may be made.

12.2 We will not and cannot charge a fee for complying with a subject access request save in exceptional circumstances described in Schedule 1.

12.3 Except in limited circumstances when complying with a subject access request we will not disclose the personal data of third parties. For this reason, personal data of third parties will be redacted from documents which are provided to the requester.

12.4 In certain circumstances, exemptions may apply which may require or allow us to withhold information requested in response to a subject access request.

12.5 We will keep records of all subject access requests and a record of why information was redacted or withheld (e.g. subject to an exemption).

13. DISCLOSURES OF INFORMATION TO THIRD PARTIES (DATA SHARING)

13.1 All personal data is held securely by us and will be treated in a confidential manner. We will only disclose personal data when we have legal grounds to do so and if we have previously informed the data subject about the possibility of similar disclosures (in a privacy notice), unless legal exemptions apply. These disclosures may include:

1. Disclosures made in accordance with a legal obligation, such as a court order or statutory duty;

2. Disclosures made in order to enforce or apply any contract with the data subject; or

3. Disclosures made to protect our rights, property, or safety of our employees, volunteers, contractors or others. This includes exchanging information for the purposes of the prevention or detection of crime

13.2 We will keep records of all information supplied in response to a request for disclosure by a third party and will carefully document any exemptions which may have been applied (including the reasons for their application). Legal advice may need to be obtained in appropriate cases.

13.3 We will abide by the ICO's statutory Data Sharing Code of Practice (or any replacement code of practice) when sharing personal data with other data controllers.

14. SECURITY OF PERSONAL DATA

14.1 Personal data will be processed in a manner that ensures that it is kept appropriately protected and secure, including from unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical and organisational measures.

14.2 We will implement appropriate technical and security measures which ensure a level of security of processing which is appropriate to the risk of processing.

In assessing the appropriateness of technical and organisational measures we shall take into account:

1. the state of the art;

2. the costs of implementation;

3. the nature, scope, context and purpose of processing;

4. the risk (of varying likelihood and severity) for the rights and freedoms of natural persons. In assessing the appropriateness of the level of security we shall, among other relevant considerations, take into account the risks that are presented by the processing involved, in particular the risks which could result from a personal data breach

14.3 We will put in place policies, measures, procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. These may include:

1. Pseudonymisation and encryption of personal data

2. Measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

3. Measures to ensure that we are able to restore availability and access to personal data in a timely manner if there is a physical or technical incident;

4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing.

14.4 The security measure we put in place include:

1. Physical Security

2. Systems Security

3. Organisational Security

15. TRANSFERRING PERSONAL DATA OUTSIDE THE EUROPEAN UNION (EU)

15.1 BMS will only transfer personal data we hold to a country outside the EU if this is permitted under the GDPR. This includes situations where we upload personal data to a cloud the servers of which are situated outside the EU.

15.2 Under the GDPR, we are permitted to transfer data outside the EU in certain circumstances. These include situations where we transfer data:

1. To a country or international organisation which the European Commission declares, by means of a decision, to be a country or international organisation which provides an adequate level of protection (provided that the relevant decision remains in force);

2. Pursuant to a contract which incorporates model contractual clauses which are issued by the European Commission or the ICO in accordance with the GDPR;
3. Pursuant to contractual clauses which are authorised by the ICO;

4. The data subject explicitly consents to the transfer, which consent shall be of the level required in section 7 of this policy and the GDPR;

5. The transfer is necessary for one of the reasons set out in Article 59 of the GDPR, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject

15.3 Satisfying one of the conditions in paragraph 15 does not eliminate the need to comply with all other requirements for processing personal data.

15.4 When we use the services of a cloud service provider (or any other data processor) which requires data to be processed outside the EU we will ensure that we satisfy one of the conditions contained in this section 15 of this policy (or alternatives provided under the GDPR) as well as comply with the requirements relating to the appointment of data processors described in section 20 of this policy.

16. DEALING WITH DATA PROTECTION BREACHES

16.1 All suspected breaches should be reported to the Data Protection Officer.

16.2 We will keep records of personal data breaches, even if we do not report them to the ICO, and such records will be such as to enable the ICO to verity our compliance with the GDPR. The records will be kept by the Data Protection Officer and will describe, as a minimum:

1. The facts relating to the personal data breach;

2. Its effects; and

3. Remedial action taken.

16.3 We are required to report all data breaches which are likely to result in a risk to any person, to the ICO. Reports will be made within 72 hours from when we become aware of the breach and the time limit starts to run from when any member of staff or contractor becomes aware of the breach and not when reported to dataprotection@bmsworldmission.org.

16.4 When a data protection breach occurs, the Data Protection Officer shall consider the following:

1. Does this policy require amending?

2. Should further guidance be issued about this policy?

3. Do any members of staff require additional training or guidance?

4. Is it appropriate to take disciplinary action?

17. RECORD KEEPING

17.1 The GDPR requires that organisations not only comply with the law but are able to show that they comply with the law.

17.2 The GDPR specifically requires that we keep, as a minimum, the following records about our processing activities:

1. The name and contact details of any joint controller, any representative and/or Data Protection Officer;

2. The purpose of the processing

3. A description of the categories of data subjects;

4. A description of the categories of personal data;

5. The categories of recipients to whom the personal data have been or will be disclosed;

6. Transfers to countries or organisations outside the EU (including their identification) and any relevant safeguards;

7. The envisaged time limits for erasure of the different data;

8. A description of security measures taken

9. Reasons for decisions taken

17.3 The GDPR also requires data processors to keep records and when appointing a data processor, we shall require them, in the contract by which they are appointed, to keep such records and to give us access to such records when we require it.

18. DATA PROTECTION BY DESIGN AND BY DEFAULT

18.1 We will implement appropriate technical and organisational measures to ensure that all personal data is processed in accordance with the GDPR, primarily the principles of data protection described in this policy. This includes having safeguards built into our systems which provide for compliance by default.

19. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

19.1 Before carrying out any data processing which is likely to result in a high risk we will carry out a Data Protection Impact Assessment (DPIA). These include situations when we process data relating to vulnerable people, trawling of data from public profiles and data transfers outside the EU. We may also conduct a DPIA in other cases when we consider it appropriate to do so. Any decision not to conduct a DPIA shall be recorded.

20. APPOINTING DATA PROCESSORS

20.1 When appointing a contractor who will process personal data on our behalf (a data processor) we will, before appointing them, carry out a due diligence exercise to ensure that the relevant processor will implement appropriate technical and organisational measures to ensure that the data processing will meet the requirements of data protection law, including keeping the data secure, and will ensure protection of the rights of data subjects. We will only appoint data processors who can provide us with sufficient guarantees that they will do so.

21. APPLICATION

21.1 Cyan International has written procedures designed to ensure this policy is implemented appropriately.

21.2 Our contracted data processors are required to comply with this policy under contract. Any breach of the policy will be taken seriously and could lead to contract enforcement action or termination of the contract. Data processors have direct obligations under the GDPR, primarily to only process data on instructions from the controller (us) and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.

22. POLICY REVIEW

22.1 This policy has been approved by the Cyan International Board of Trustees which is responsible for ensuring that we comply with all our legal obligations. It sets out the legal rules which apply whenever we obtain, store or use personal data.

22.2 Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred tovsteven@cyanint.org.

The Trustees will directly or through delegated authority:

1. Keep the content and effectiveness of this policy under review;

2. Oversee compliance with the policy;

3. Keep a record of all data security incidents or breaches and investigate in appropriate detail;

4. Provide or arrange training and guidance for staff;

The Cyan Data Protection Officer will act as our nominated contact with the ICO.

References in this policy to the Data Protection Officer shall be construed as references to the Data Protection Officer or such other person as the Data Protection Officer may appoint to act on his or her behalf.

22.3 From time to time we may need to make changes to this policy or guidance in line with current operational practices and/or legislation.

22.4 Any questions, ideas or concerns about the operation of this policy or recommendations for additions or amendments should be referred to vsteven@cyanint.org.

We reserve the right to change this policy at any time. Any amended versions of this policy will take effect from the time they are uploaded to our website. Where appropriate, we will notify data subjects of those changes by mail or by email.

The Data Protection Officer (DPO): Val Steven

Appendix 1

Cyan International Privacy Notice

Introduction

We, Cyan International, are the 'controllers' of the information which we collect about you ('personal data'). Being controllers of your personal data, we are responsible for how your data is processed. The word 'process' covers most things that can be done with personal data, including collection, storage, use and destruction of that data.

This notice explains why and how we process your data, and explains the rights you have around your data, including the right to access it, and to object to the way it is processed. Please see the section on 'Your rights as a data subject' for more information.

Our Data Protection contact point is vsteven@cyanint.org if you have any queries about this notice or anything related to data protection.

Where employed by Cyan International within the EU or UK, Cyan collects and processes personal data relating to you to manage the employment relationship.

Personal data

'Personal data' is any information that relates to a living, identifiable person. This data can include your name, contact details, and other information we gather as part of our relationship with you.

It can also include 'special categories' of data, which is information about a person's race or ethnic origin, religious, political or other beliefs, physical or mental health, trade union membership, genetic or biometric data, sex life or sexual orientation. The collection and use of these types of data is subject to strict controls. Similarly, information about criminal convictions and offences is also limited in the way it can be processed.

Cyan International is committed to protecting your personal data, whether it is 'special categories' or not, and we only process data if we need to for a specific purpose, as explained below.

We collect your personal data mostly through our contact with you, and the data is usually provided by you, but in some instances, we may receive data about you from other people/organisations. We will explain when this might happen in this Notice.

Your data and how and why we process it

In general terms, we process your data in order to enter into an employment contract with you, to meet our obligations under that contract, to pay you in accordance with your contract and to administer benefits and entitlements.

In some cases, we need to process data to comply with our legal obligations, for example we are required to check your entitlement to work in the UK, to deduct tax and other amounts required by HMRC, to

comply with health and safety law and to enable you to take periods of leave to which you are entitled. For certain positions it is necessary to carry out criminal records checks.

In other cases, we have a legitimate interest in processing personal data before, during and after the end of the employment relationship. This is needed for a number of essential purposes including to:

- run recruitment, selection and promotion processes
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights
- operate and keep a record of disciplinary and grievance processes, to support reasonable levels of conduct within the workplace
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and team management purposes
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that you receive the pay or other benefits to which you are entitled
- obtain occupational health advice, to ensure that we comply with duties in relation to individuals with disabilities, meet our obligations under health and safety law, and ensure that you receive the pay or other benefits to which you are entitled
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective management of our teams, to ensure that we comply with duties in relation to leave entitlement, and to ensure that you are receiving the pay or other benefits to which you are entitled
- ensure effective general HR and business administration
- provide references on request for current or former employees
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities, long term ill health issues and for health and safety purposes).

Where Cyan International processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal

opportunities monitoring. Data that Cyan International uses for these purposes is collected with the express consent of employees, which can be withdrawn at any time. You are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so. Where a role has an occupational requirement for an individual to be a committed Christian we will also hold data related to your religion and beliefs.

At times, we may further process data which we have already collected. We will only do this if the new purpose for processing it further is compatible with the original purpose that the data was collected for. We will tell you about any further processing before carrying it out.

The specific information that Cyan International may hold on you will include:

- your name, address and contact details, including email address and telephone number
- your date of birth and gender
- the terms and conditions of your employment
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with Cyan International
- information about your pay, including entitlement to benefits such as pensions or insurance cover, and details of statutory deductions such as tax, national insurance, student loans and other
- details of your bank account and national insurance number
- information about your marital status, next of kin, dependants and emergency contacts
- information about your nationality and entitlement to work in the UK or another overseas country
- information related to your application to work overseas including copies of your passports, visas, travel arrangements, and any overseas partner specific recruitment process documents
- information related to your secondment to work for an overseas partner
- information about your criminal record where this is relevant to your employment
- details of your schedule (days of work and working hours) and attendance at work
- details of periods of leave taken by you, including holiday, sickness absence, family and other leave, and the reasons for the leave

- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence

- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence

- information about medical or health conditions, including whether or not you have a disability for which BMS needs to make reasonable adjustments; and

- equal opportunities monitoring information, including information (if you have provided it) about your ethnic origin, sexual orientation, health and religion or belief

Personal data received from third parties

This is a list of your personal data that we may receive from other people or organisations. The list is not exhaustive but covers the type of documents we may need to hold on record.

Data	Source
Personal references	Appointed referees
Tax coding	HMRC
Payroll deductions such as student loans, court orders or other statutory deductions	HMRC

Who we share your data with

For some processing purposes we share your data with third parties. The list is not exhaustive but covers the type of documents we may need to share with third parties. This is a list of the information we may share with external recipients, and for what purpose:

Recipients of your data	Purpose for sharing
HMRC	Payment of tax / NI
BMS Pension Trustee	Payment of pension contribution
Life assurance provider	Arrangement of life cover
Cyan Int auditor	Statutory audit
Access Consortium	Payroll calculations
Travel Agents/Flight bookers	To enable your travel
Embassy and consulates	To acquire your visa
Travel Health Clearance specialists	To ensure you are fit to travel/work overseas
Criminal check agency	To obtain clearance for you to work with vulnerable individuals in certain roles

How we store your data

Your personal data may be held temporarily in hard copy and then in electronic formats.
Electronic data, including emails, is stored on our servers or our service provider's servers, which are located and backed up in the UK/European Union.

How long we keep your data

Information about how long we process your data for can be found in the appendix below. Some retention periods are based on legal requirements while others take into account practical needs to keep the data.
Once the applicable retention period expires, unless we are legally required to keep the data longer, or there are important and justifiable reasons why we should keep it, we will securely delete the data.

Your rights as a data subject

As a data subject, you have the following rights in relation to your personal data processed by us:

- To be informed about how your data is handled
- To gain access to your personal data
- To have errors or inaccuracies in your data changed;
- To have your personal data erased, in limited circumstances
- To object to the processing of your personal data for marketing purposes or when the processing is based on the public interest or other legitimate interests
- To restrict the processing of your personal data, in limited circumstances
- To obtain a copy of some of your data in a commonly used electronic form, in limited circumstances
- Rights around how you are affected by any profiling or automated decisions

Withdrawing consent

If we are relying on your consent to process your data, you may withdraw your consent at any time by contacting vsteven@cyanint.org.

Exercising your rights, queries and complaints

If you wish to see your file please contact the Cyan Head of Operations by email to arrange a time when you will be given access in a private room. This will be arranged within four weeks of the request. Our Data Protection Policy allows us to charge for repeat requests of the same data or for refusal of unreasonable requests.

Complaints to the Information Commissioner

You have a right to complain to the Information Commissioner's Office (ICO) about the way in which we process your personal data. You can make a complaint on the ICO's website https://ico.org.uk/.

Data Retention Policy for HR records

Data	Retention period
HR file	Up to 7 years from leave date
Payroll records	Up to 7 years from leave date
References given to prospective employers	Up to 7 years from leave date
Executive director HR file	Indefinite
Information of safeguarding concern	Indefinite
Summary record of name, NI number, date of birth, employment dates and positions held	Indefinite

Cyan International is registered as a charity in England and Wales (1129603).