**Customer Vendor Data Processing Agreement**

**Background:**

The Vendor provides certain services to Customer. The parties have agreed that this Agreement shall govern the processing of any Personal Data by the Vendor in connection with the Vendor Agreement(s). This Agreement shall be effective as of May 25, 2018 and shall remain in effect for the duration of the Vendor Agreement and shall terminate upon termination or expiration of the Vendor Agreement.

* 1. **Definitions and interpretation**
		1. In this Agreement, unless the context otherwise requires:

**"Data Protection Laws"** means any laws and regulations in any relevant jurisdiction relating to privacy or the use or processing of data relating to natural persons, including: (a) EU Directives 95/46/EC and 2002/58/EC (as amended by 2009/139/EC) and any legislation implementing or made pursuant to such directives, including (in the UK) the Data Protection Act 1998 (the **"DPA"**) and the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (b) from 25 May 2018, EU Regulation 2016/679 (**"GDPR"**); and (c) any laws or regulations ratifying, implementing, adopting, supplementing or replacing GDPR; and (d) any guidance or codes of practice issued by a governmental or regulatory body or authority in relation to compliance with the foregoing; in each case, to the extent in force, and as such are updated, amended or replaced from time to time.

**"Data Controller"** and "**Data Processor**" have the meanings set out in the DPA until 25 May 2018, and thereafter the meaning given to the term "controller" and "processor" (respectively) in Article 4 of GDPR.

**"DP Regulator"** means any governmental or regulatory body or authority with responsibility for monitoring or enforcing compliance with the Data Protection Laws.

**"Data Subject Request"** means a request from a Data Subject to exercise its rights under the Data Protection Laws in respect of that Data Subject's Personal Data.

**"Permitted Region"** means the United Kingdom and the European Economic Area.

**"Security Breach"** means any actual loss, unauthorised or unlawful processing, destruction, damage, or alteration, or unauthorised disclosure of, or access to the Customer Data.

**"Standard Contractual Clauses"** means the standard contractual clauses set out in the European Commission's Decision 2010/87/EU of 5 February 2010 for the transfer of Personal Data to processors established in third countries and attached hereto as Appendix 4.

**"Sub-Processor"** means any subcontractor (including any affiliates of the Vendor) appointed by the Vendor to process Customer Data.

**"Customer Data"** any Personal Data processed in connection with a Vendor Agreement.

**"Vendor Agreement"** means any agreement or agreements entered by Customer and the Vendor from time to time, under which the Vendor provides services to Customer.

* + 1. In this Agreement, the terms **"Data Subject"**, **"Personal Data"**, **"process"**, **"processing"**, **"transfer"** (in the context of transfers of Personal Data) and **"technical and organisational measures"** shall have the meanings and otherwise be interpreted in accordance with applicable Data Protection Laws.
	1. **Compliance with Data Protection Laws**
		1. The Vendor shall comply with the Data Protection Laws as they apply to Data Processors.
		2. The Vendor shall maintain records of all processing operations under its responsibility that contain at least the minimum information required by the Data Protection Laws as they apply to Data Processors, and shall make such information available to any DP Regulator on request.
	2. **Processing and security**
		1. The Vendor agrees that it shall only process the types of Customer Data, and only in respect of the categories of Data Subjects, and only for the nature and purposes of processing and duration, as is set out in Appendix 1 to this Agreement.
		2. In processing Customer Data, the Vendor shall:

#### process the Customer Data only in accordance with Customer's written instructions from time to time (including those set out in this Agreement and the Vendor Agreement) unless it is otherwise required by applicable law (in which case, unless such law prohibits such notification on important grounds of public interest, the Vendor shall notify Customer of the relevant legal requirement before processing the Customer Data);

#### not process the Customer Data for any purpose other than those set out in this Agreement or otherwise expressly authorized by Customer;

#### notify Customer within twenty four (24) hours if it receives a Data Subject Request in respect of Customer Data;

#### provide Customer with its full cooperation and assistance in relation to any Data Subject Request in respect of Customer Data;

#### not disclose any Customer Data to any Data Subject or to a third party (including any subcontractor or affiliate) other than at the written request of Customer or as expressly provided for in this Agreement;

#### taking into account:

##### the state of the art;

##### the nature, scope, context and purposes of the processing; and

##### the risk and severity of potential harm,

protect the Customer Data by ensuring that it has in place appropriate technical and organisational measures, including measures to protect the Customer Data against the risks of a Security Breach and including without limitation the measures set out in Appendix 3; and

#### ensure that only persons authorised by the Vendor process Customer Data and that such persons are (i) subject to binding obligations to maintain the confidentiality of the Customer Data; and (ii) trained on both (1) the requirements of the Data Protection Laws, and (2) their obligations in respect of Customer Data under this Agreement.

* + 1. The Vendor shall, without undue delay (and in any event within twenty-four (24) hours) after discovering any Security Breach or any failure or defect in security which leads, or might reasonably be expected to lead, to a Security Breach (together a "**Security Issue**") notify Customer of the same.
		2. Where a Security Issue arises, the Vendor shall:

#### as soon as reasonably practicable, provide Customer with full details of the Security Issue, the actual or expected consequences of it, and the measures taken or proposed to be taken to address or mitigate it;

#### co-operate with Customer, and provide Customer with all reasonable assistance in relation to the Security Issue; and

#### unless required by applicable law, not make any notifications to a DP Regulator or any Data Subjects about the Security Issue without Customer's prior written consent (not to be unreasonably withheld or delayed).

* 1. **Return or destruction of Customer Data**
		1. Subject to clause 4.4, the Vendor shall (at Customer's option) return or irretrievably delete all Customer Data in its control or possession when it no longer requires such Customer Data to exercise or perform its rights or obligations under this Agreement, and in any event on expiry or termination of this Agreement.
		2. The deletion or destruction of Customer Data shall be documented by the Vendor. Upon request, the Vendor shall provide Customer with the documentation.
		3. The Vendor shall keep (for the applicable retention period) all documents necessary to prove compliance of the processing of Customer Data with contractual and statutory obligations of the Vendor. In this case, the Vendor shall treat the Customer Data as confidential.
		4. To the extent that the Vendor is required by applicable law to retain all or part of the Customer Data (the **"Retained Data"**), the Vendor shall:

#### notify Customer that it is required to retain the Customer Data, including in its notification and explanation of the applicable laws which require it to retain the Retained Data;

#### cease all processing of the Retained Data other than as required by the applicable law;

#### keep confidential all such Retained Data in accordance with the relevant Vendor Agreement; and

#### continue to comply with the provisions of this Agreement in respect of such Retained Data.

* 1. **Audit**
		1. The Vendor shall comply with all requests from Customer (and its auditors, and its and their internal or external representatives) to access and inspect the Vendor's (and its Sub-Processors') premises, records and personnel relevant to any processing of Customer Data, in each case to enable Customer to audit and verify that the Vendor (and its Sub-Processors) is complying fully with its obligations under this Agreement and under the Data Protection Laws in relation to Customer Data.
		2. The Vendor shall provide such information, cooperation and assistance in relation to any request made by Customer (or its auditors, or its or their representatives) under clause 5.1 as Customer may reasonably require.
	2. **Cooperation and assistance**
		1. The Vendor shall promptly cooperate with Customer, and promptly provide such information and assistance as Customer may reasonably require, to enable Customer to:

#### comply with Customer's obligations under the Data Protection Laws (including Articles 32-36 of the GDPR) in respect of Customer Data; and

#### deal with and respond to all investigations and requests for information relating to the Customer Data from any DP Regulator.

* + 1. If the Vendor receives any complaint, notice or communication from a DP Regulator or other third party (excluding a Data Subject Request) which relates directly or indirectly to Customer Data or to either party's compliance with the Data Protection Laws, it shall notify Customer as soon as reasonably practicable.
		2. Where any provision of this Agreement places an obligation on the Vendor, that obligation shall be construed as an obligation on the Vendor to procure that all its Sub-Processors, and its own and its Sub-Processors’ personnel, comply with such obligation.
	1. **Sub-Processors**
		1. The Vendor shall not appoint any Sub-Processor other than in accordance with this clause 7.
		2. Customer hereby consents to the Vendor's use of the Sub-Processors set out in Appendix 2 of this Agreement. If the Vendor wishes to appoint any further Sub-Contractors, it shall notify Customer in writing as soon as possible following the appointment of any such Sub-Contractor. If Customer objects to the appointment of such Sub-Processor, Customer shall notify the Vendor within 30 days of receiving notification of their appointment (a "**Sub-Processor Objection Notice**"). If Customer does not provide a Sub-Processor Notice within the 30 day time period, then it shall be deemed to have consented to the appointment of such Sub-Processor.
		3. If Customer provides a Sub-Processor Objection Notice, or if Customer has a bona fide, reasonable belief that a Sub-Processor appointed by the Vendor poses a risk to data subjects, then the Vendor shall use all reasonable endeavours to provide the services under the relevant Vendor Agreement without using the relevant Sub-Processor. In the event that Customer considers that the Vendor is unable to provide adequate assurances, without prejudice to any other rights or remedies it may have, Customer may terminate the relevant Vendor Agreement on written notice, and shall be refunded pro-rata any amounts for services which it has paid for, but which have not yet been provided by the Vendor.
		4. If the Vendor appoints a Sub-Processor, the Vendor shall ensure that:

#### such Sub-Processor shall only process Customer Data in order to perform one or more of the Vendor's obligations under the Vendor Agreement; and

#### it enters into a written agreement with that Sub-Processor, prior to any processing by the Sub-Processor, requiring the Sub-Processor to:

##### process Customer Data only in accordance with the written instructions of the Vendor or Customer; and

##### complies with obligations relating to data protection which are equivalent in all material respects to those imposed on the Vendor in this Agreement.

* + 1. Notwithstanding the appointment of a Sub-Processor, the Vendor is responsible and liable to Customer for any processing by the Sub-Processor in breach of this Agreement.
	1. **Transfer of Personal Data**
		1. The Vendor shall not process any Customer Data, or otherwise transfer or access any Customer Data, outside of the Permitted Region without the express prior written consent of Customer.
		2. Customer's consent under clause 8.1 shall be conditional upon the Vendor ensuring there is adequate protection and appropriate safeguards for such Customer Data in accordance with applicable Data Protection Laws when it is transferred or accessed outside of the Permitted Region by entering into the Standard Contractual Clauses with Customer, as set forth in Appendix 4.
		3. If Customer authorises the Vendor to transfer Customer Data outside the Permitted Region pursuant to clause 8.1 and either (a) the means by which adequate protection for the transfer is achieved ceases to be valid, or (b) any DP Regulator (or other supervisory or regulatory authority) requires transfers of Personal Data pursuant to such Standard Contractual Clauses to be suspended, then Customer may (at its discretion) require the Vendor immediately to cease transfers of Personal Data and delete or return all Personal Data previously transferred.
	2. **Indemnity**

The Vendor shall indemnify and keep indemnified at its own expense Customer against all claims, liabilities, damages, administrative fines, costs or expenses incurred by Customer or for which Customer may become liable due to any failure by the Vendor or its Sub-Processors, subcontractors, agents or personnel to comply with any of its obligations under this Agreement or under the Data Protection Laws.

* 1. **General**
		1. Except as set out in this Agreement, the provisions of the Vendor Agreement shall remain unchanged and shall continue in force.
		2. No variation of this Agreement shall be valid unless it is in writing (which excludes email) and signed by or on behalf of each of the parties by its respective authorised representatives.
		3. No single or partial exercise, or failure or delay in exercising any right, power or remedy by any party shall constitute a waiver by that party of, or impair or preclude any further exercise of, that or any right, power or remedy arising under this Agreement or otherwise.
		4. Excluding conflict of laws rules, this Agreement shall be governed by and construed under the laws of the State of Washington, U.S. All disputes arising out of or in relation to this Agreement shall be submitted to the exclusive jurisdiction of the courts of Seattle, Washington. Nothing in this section shall restrict Customer’s right to bring an action against you in the jurisdiction where your place of business is located.

Signed for and on behalf of
**Customer**

Signature: ……………………………………….

Name: ………………………………………

Position: ………………………………………

Date: ………………………………………

Signed for and on behalf of
**Vendor**

Signature: ……………………………………….

Name: ………………………………………

Position: ………………………………………

Date: ………………………………………

**Appendix 1**

**Details of Processing**

The processing activities carried out by the Vendor under this Agreement may be described as follows:

* 1. **Subject matter and duration of Processing**

*The subject matter of processing is information and data uploaded by Customer employees and customers into Vendor’s system. Processing shall only take place so long as it is required under the Vendor Agreement and so long as the Vendor Agreement remains in effect.*

* 1. **Nature and purpose of Processing**

*Computing and data storage as is necessary to provide services as described in the Vendor Agreement.*

* 1. **Type of Personal Data and categories of Data Subjects**

*Business information and data that is uploaded by Customer employees and Customer customers so that Customer may provide technical support to customers for its products.*

**Appendix 2**

**Approved Sub-Processors**

Amazon Web Services

**Appendix 3**

**Technical and organisational security measures**

# CyanGate Data Protection Policy

# Introduction

# CyanGate, LLC is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

# We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

# This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

# Definitions

|  |  |
| --- | --- |
| **Business purposes** | The purposes for which personal data may be used by us:Personnel, administrative, financial, regulatory, payroll and business development purposes.*Business purposes include the following:**- Compliance with our legal, regulatory and corporate governance obligations and good practice**- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests**- Ensuring business policies are adhered to (such as policies covering email and internet use)**- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking**- Investigating complaints* *- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments**- Monitoring staff conduct, disciplinary matters**- Marketing our business**- Improving services* |

|  |  |
| --- | --- |
| **Personal data** | ‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.* |
| **Special categories of personal data** | Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy. |
| **Data controller** | ‘Data controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law. |
| **Data processor** | ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. |
| **Processing** | ‘Processing’ means 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| **Supervisory authority** | This is the national body responsible for data protection. The supervisory authority for our organization is the **Information Commissioners Office**. |

# Scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

As our data protection officer (DPO), **Burak Fenercioglu** has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary.

Burak Fenercioglu

burakf@cyangate.com

Phone: +1-833-326-9778

# The principles

CyanGate, LLC shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles. The Principles are:

**1. Lawful, fair and transparent**

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

**2. Limited for its purpose**

Data can only be collected for a specific purpose.

**3. Data minimisation**

Any data collected must be necessary and not excessive for its purpose.

**4. Accurate**

The data we hold must be accurate and kept up to date.

**5. Retention**

We cannot store data longer than necessary.

**6. Integrity and confidentiality**

The data we hold must be kept safe and secure.

Accountability and transparency

We must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. You are responsible for keeping a written record of how all the data processing activities you are responsible for comply with each of the Principles. This must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

* Fully implement all appropriate technical and organizational measures
* Maintain up to date and relevant documentation on all processing activities
* Conducting Data Protection Impact Assessments
* Implement measures to ensure privacy by design and default, including:
	+ Data minimisation
	+ Pseudonymisation
	+ Transparency
	+ Allowing individuals to monitor processing
	+ Creating and improving security and enhanced privacy procedures on an ongoing basis

# Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals’ rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased

Controlling vs. processing data

CyanGate, LLC is classified as a data processor. We must maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully processing data.

As a data processor, we must comply with our contractual obligations and act only on the documented instructions of the data controller. If we at any point determine the purpose and means of processing out with the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller. As a data processor, we must:

* Not use a sub-processor without written authorisation of the data controller
* Co-operate fully with the ICO or other supervisory authority
* Ensure the security of the processing
* Keep accurate records of processing activities
* Notify the controller of any personal data breaches

If you are in any doubt about how we handle data, contact the DPO for clarification.

Lawful basis for processing data

We must establish a lawful basis for processing data. Ensure that any data you are responsible for managing has a written lawful basis approved by the DPO. It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent**

We hold recent, clear, explicit, and defined consent for the individual’s data to be processed for a specific purpose.

1. **Contract**

The processing is necessary to fulfil or prepare a contract for the individual.

1. **Legal obligation**

We have a legal obligation to process the data (excluding a contract).

1. **Vital interests**

Processing the data is necessary to protect a person’s life or in a medical situation.

1. **Public function**

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

1. **Legitimate interest**

The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual’s personal data which overrides the legitimate interest.

Deciding which condition to rely on

If you are making an assessment of the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means.

Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

Consider the following factors and document your answers:

* What is the purpose for processing the data?
* Can it reasonably be done in a different way?
* Is there a choice as to whether or not to process the data?
* Who does the processing benefit?
* After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
* What is the impact of the processing on the individual?
* Are you in a position of power over them?
* Are they a vulnerable person?
* Would they be likely to object to the processing?
* Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the DPO.

# Special categories of personal data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person’s fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual’s:

* race
* ethnic origin
* politics
* religion
* trade union membership
* genetics
* biometrics (where used for ID purposes)
* health
* sexual orientation

In most cases where we process special categories of personal data, we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

# Responsibilities

Our responsibilities

* Analyzing and documenting the type of personal data we hold
* Checking procedures to ensure they cover all the rights of the individual
* Identify the lawful basis for processing data
* Ensuring consent procedures are lawful
* Implementing and reviewing procedures to detect, report and investigate personal data breaches
* Store data in safe and secure ways
* Assess the risk that could be posed to individual rights and freedoms should data be compromised

Your responsibilities

* Fully understand your data protection obligations
* Check that any data processing activities you are dealing with comply with our policy and are justified
* Do not use data in any unlawful way
* Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
* Comply with this policy at all times
* Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

Responsibilities of the Data Protection Officer

* Keeping the board updated about data protection responsibilities, risks and issues
* Reviewing all data protection procedures and policies on a regular basis
* Arranging data protection training and advice for all staff members and those included in this policy
* Answering questions on data protection from staff, board members and other stakeholders
* Responding to individuals such as clients and employees who wish to know which data is being held on them by us
* Checking and approving with third parties that handle the company’s data any contracts or agreement regarding data processing

Responsibilities of the IT Manager

* Ensure all systems, services, software and equipment meet acceptable security standards
* Checking and scanning security hardware and software regularly to ensure it is functioning properly
* Researching third-party services, such as cloud services the company is considering using to store or process data

Responsibilities of the Marketing Manager

* Approving data protection statements attached to emails and other marketing copy
* Addressing data protection queries from clients, target audiences or media outlets
* Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company’s Data Protection Policy

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Data security

You must keep personal data secure against loss or misuse. Where other organizations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organizations.

Storing data securely

* In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
* Printed data should be shredded when it is no longer needed
* Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a [password manager](http://cybersecurityzen.com/cybersecurity/keep-data-safe-rise-password-managers-1654/) to create and store their passwords.
* Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
* The DPO must approve any cloud used to store data
* Servers containing personal data must be kept in a secure location, away from general office space
* Data should be regularly backed up in line with the company’s backup procedures
* Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
* All servers containing sensitive data must be approved and protected by security software
* All possible technical measures must be put in place to keep data secure

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the DPO.

# Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

**1. Right to be informed**

* Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
* Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

**2. Right of access**

* Enabling individuals to access their personal data and supplementary information
* Allowing individuals to be aware of and verify the lawfulness of the processing activities

**3. Right to rectification**

* We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
* This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

**4. Right to erasure**

* We must delete or remove an individual’s data if requested and there is no compelling reason for its continued processing.

**5. Right to restrict processing**

* We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
* We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

**6. Right to data portability**

* We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
* We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

**7. Right to object**

* We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
* We must respect the right of an individual to object to direct marketing, including profiling.
* We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

**8. Rights in relation to automated decision making and profiling**

* We must respect the rights of individuals in relation to automated decision making and profiling.
* Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

# Privacy notices

When to supply a privacy notice

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which mean within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

What to include in a privacy notice

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children

The following information must be included in a privacy notice to all data subjects:

* Identification and contact information of the data controller and the data protection officer
* The purpose of processing the data and the lawful basis for doing so
* The legitimate interests of the controller or third party, if applicable
* The right to withdraw consent at any time, if applicable
* The category of the personal data (only for data not obtained directly from the data subject)
* Any recipient or categories of recipients of the personal data
* Detailed information of any transfers to third countries and safeguards in place
* The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
* The right to lodge a complaint with the ICO, and internal complaint procedures
* The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
* Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
* Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

# Subject Access Requests

What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

How we deal with subject access requests

We must provide an individual with a copy of the information the request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the DPO before extending the deadline.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

Data portability requests

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the DPO first.

# Right to erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

* Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
* Where consent is withdrawn
* Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
* The personal data was unlawfully processed or otherwise breached data protection laws
* To comply with a legal obligation
* The processing relates to a child

How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

* To exercise the right of freedom of expression and information
* To comply with a legal obligation for the performance of a public interest task or exercise of official authority
* For public health purposes in the public interest
* For archiving purposes in the public interest, scientific research, historical research or statistical purposes
* The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

* We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
* The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

The right to restrict automated profiling or decision making

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

* It is necessary for the entry into or performance of a contract.
* Based on the individual’s explicit consent.
* Otherwise authorised by law.

In these circumstances, we must:

* Give individuals detailed information about the automated processing.
* Offer simple ways for them to request human intervention or challenge any decision about them.
* Carry out regular checks and user testing to ensure our systems are working as intended.

# Third parties

Using third party controllers and processors

As a data processor, we must have written contracts in place with any third party data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Contracts

Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

* Acting only on written instructions
* Those involved in processing the data are subject to a duty of confidence
* Appropriate measures will be taken to ensure the security of the processing
* Sub-processors will only be engaged with the prior consent of the controller and under a written contract
* The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
* The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
* Delete or return all personal data at the end of the contract
* Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
* Nothing will be done by either the controller or processor to infringe on GDPR.

# Criminal offence data

### Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. You must have approval from the DPO prior to carrying out a criminal record check.

# Audits, monitoring and training

Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must conduct a regular data audit as defined by the DPO and normal procedures.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. CyanGate, LLC will keep this policy under review and amend or change it as required. You must notify the DPO of any breaches of this policy. You must comply with this policy fully and at all times.

Training

You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

If you require additional training on data protection matters, contact the DPO.

# Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. CyanGate, LLC has a legal obligation to report any data breaches to a Lead Supervisory Authority (LSA) within 10 business days.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

* Investigate the failure and take remedial steps if necessary
* Maintain a register of compliance failures
* Notify the LSA of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Please refer to our **Information Security Breach Report** for our reporting procedure.

Failure to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organization at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

**APPENDIX 4 - Standard Contractual Clauses (processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity identified as « Customer » in the Agreement,

(the data **exporter**)

And

The entity identified as “Vendor” in the Agreement,

(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

*Clause 1*

***Definitions***

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[[1]](#footnote-1);

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law****'*** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

*Clause 2*

***Details of the transfer***

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

*Clause 3*

***Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

*Clause 4*

***Obligations of the data exporter***

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

*Clause 5*

***Obligations of the data importer[[2]](#footnote-2)***

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

*Clause 6*

***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

*Clause 7*

***Mediation and jurisdiction***

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

*Clause 8*

***Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

*Clause 9*

***Governing Law***

The Clauses shall be governed by English law.

*Clause 10*

***Variation of the contract***

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

*Clause 11*

***Subprocessing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[[3]](#footnote-3). Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by English laws.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

*Clause 12*

***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**ANNEX 1 to the Standard Contractual Clauses**

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

**Data exporter**

The data exporter is (please specify briefly your activities relevant to the transfer):

Customer International, Unlimited Company ………………………………………………………………………………………………

**Data importer**

The data importer is (please specify briefly activities relevant to the transfer):

CyanGate LLC provides backup electronic file storage in the cloud ………………………………………………………………………………………………………………………………………………………………………………………………

**Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

Customer customers and employees

**Categories of data**

The personal data transferred concern the following categories of data (please specify):

Data vizualizations and business analytics data

**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify):

………………………………………………………………………………………………………………………………………………………………………………………………

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

Electronic storage

**ANNEx 2 to the Standard Contractual Clauses**

This Appendix forms part of the Clauses and must be completed and signed by the parties.

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

# CyanGate Data Protection Policy

# Introduction

# CyanGate, LLC is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

# We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

# This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

# Definitions

|  |  |
| --- | --- |
| **Business purposes** | The purposes for which personal data may be used by us:Personnel, administrative, financial, regulatory, payroll and business development purposes.*Business purposes include the following:**- Compliance with our legal, regulatory and corporate governance obligations and good practice**- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests**- Ensuring business policies are adhered to (such as policies covering email and internet use)**- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking**- Investigating complaints* *- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments**- Monitoring staff conduct, disciplinary matters**- Marketing our business**- Improving services* |

|  |  |
| --- | --- |
| **Personal data** | ‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.* |
| **Special categories of personal data** | Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy. |
| **Data controller** | ‘Data controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law. |
| **Data processor** | ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. |
| **Processing** | ‘Processing’ means 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| **Supervisory authority** | This is the national body responsible for data protection. The supervisory authority for our organization is the **Information Commissioners Office**. |

# Scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

As our data protection officer (DPO), **Burak Fenercioglu** has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary.

Burak Fenercioglu

burakf@cyangate.com

Phone: +1-833-326-9778

# The principles

CyanGate, LLC shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles. The Principles are:

**1. Lawful, fair and transparent**

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

**2. Limited for its purpose**

Data can only be collected for a specific purpose.

**3. Data minimisation**

Any data collected must be necessary and not excessive for its purpose.

**4. Accurate**

The data we hold must be accurate and kept up to date.

**5. Retention**

We cannot store data longer than necessary.

**6. Integrity and confidentiality**

The data we hold must be kept safe and secure.

Accountability and transparency

We must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. You are responsible for keeping a written record of how all the data processing activities you are responsible for comply with each of the Principles. This must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

* Fully implement all appropriate technical and organizational measures
* Maintain up to date and relevant documentation on all processing activities
* Conducting Data Protection Impact Assessments
* Implement measures to ensure privacy by design and default, including:
	+ Data minimisation
	+ Pseudonymisation
	+ Transparency
	+ Allowing individuals to monitor processing
	+ Creating and improving security and enhanced privacy procedures on an ongoing basis

# Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals’ rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased

Controlling vs. processing data

CyanGate, LLC is classified as a data processor. We must maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully processing data.

As a data processor, we must comply with our contractual obligations and act only on the documented instructions of the data controller. If we at any point determine the purpose and means of processing out with the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller. As a data processor, we must:

* Not use a sub-processor without written authorisation of the data controller
* Co-operate fully with the ICO or other supervisory authority
* Ensure the security of the processing
* Keep accurate records of processing activities
* Notify the controller of any personal data breaches

If you are in any doubt about how we handle data, contact the DPO for clarification.

Lawful basis for processing data

We must establish a lawful basis for processing data. Ensure that any data you are responsible for managing has a written lawful basis approved by the DPO. It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent**

We hold recent, clear, explicit, and defined consent for the individual’s data to be processed for a specific purpose.

1. **Contract**

The processing is necessary to fulfil or prepare a contract for the individual.

1. **Legal obligation**

We have a legal obligation to process the data (excluding a contract).

1. **Vital interests**

Processing the data is necessary to protect a person’s life or in a medical situation.

1. **Public function**

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

1. **Legitimate interest**

The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual’s personal data which overrides the legitimate interest.

Deciding which condition to rely on

If you are making an assessment of the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means.

Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

Consider the following factors and document your answers:

* What is the purpose for processing the data?
* Can it reasonably be done in a different way?
* Is there a choice as to whether or not to process the data?
* Who does the processing benefit?
* After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
* What is the impact of the processing on the individual?
* Are you in a position of power over them?
* Are they a vulnerable person?
* Would they be likely to object to the processing?
* Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the DPO.

# Special categories of personal data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person’s fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual’s:

* race
* ethnic origin
* politics
* religion
* trade union membership
* genetics
* biometrics (where used for ID purposes)
* health
* sexual orientation

In most cases where we process special categories of personal data, we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

# Responsibilities

Our responsibilities

* Analyzing and documenting the type of personal data we hold
* Checking procedures to ensure they cover all the rights of the individual
* Identify the lawful basis for processing data
* Ensuring consent procedures are lawful
* Implementing and reviewing procedures to detect, report and investigate personal data breaches
* Store data in safe and secure ways
* Assess the risk that could be posed to individual rights and freedoms should data be compromised

Your responsibilities

* Fully understand your data protection obligations
* Check that any data processing activities you are dealing with comply with our policy and are justified
* Do not use data in any unlawful way
* Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
* Comply with this policy at all times
* Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

Responsibilities of the Data Protection Officer

* Keeping the board updated about data protection responsibilities, risks and issues
* Reviewing all data protection procedures and policies on a regular basis
* Arranging data protection training and advice for all staff members and those included in this policy
* Answering questions on data protection from staff, board members and other stakeholders
* Responding to individuals such as clients and employees who wish to know which data is being held on them by us
* Checking and approving with third parties that handle the company’s data any contracts or agreement regarding data processing

Responsibilities of the IT Manager

* Ensure all systems, services, software and equipment meet acceptable security standards
* Checking and scanning security hardware and software regularly to ensure it is functioning properly
* Researching third-party services, such as cloud services the company is considering using to store or process data

Responsibilities of the Marketing Manager

* Approving data protection statements attached to emails and other marketing copy
* Addressing data protection queries from clients, target audiences or media outlets
* Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company’s Data Protection Policy

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Data security

You must keep personal data secure against loss or misuse. Where other organizations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organizations.

Storing data securely

* In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
* Printed data should be shredded when it is no longer needed
* Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a [password manager](http://cybersecurityzen.com/cybersecurity/keep-data-safe-rise-password-managers-1654/) to create and store their passwords.
* Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
* The DPO must approve any cloud used to store data
* Servers containing personal data must be kept in a secure location, away from general office space
* Data should be regularly backed up in line with the company’s backup procedures
* Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
* All servers containing sensitive data must be approved and protected by security software
* All possible technical measures must be put in place to keep data secure

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the DPO.

# Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

**1. Right to be informed**

* Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
* Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

**2. Right of access**

* Enabling individuals to access their personal data and supplementary information
* Allowing individuals to be aware of and verify the lawfulness of the processing activities

**3. Right to rectification**

* We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
* This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

**4. Right to erasure**

* We must delete or remove an individual’s data if requested and there is no compelling reason for its continued processing.

**5. Right to restrict processing**

* We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
* We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

**6. Right to data portability**

* We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
* We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

**7. Right to object**

* We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
* We must respect the right of an individual to object to direct marketing, including profiling.
* We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

**8. Rights in relation to automated decision making and profiling**

* We must respect the rights of individuals in relation to automated decision making and profiling.
* Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

# Privacy notices

When to supply a privacy notice

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which mean within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

What to include in a privacy notice

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children

The following information must be included in a privacy notice to all data subjects:

* Identification and contact information of the data controller and the data protection officer
* The purpose of processing the data and the lawful basis for doing so
* The legitimate interests of the controller or third party, if applicable
* The right to withdraw consent at any time, if applicable
* The category of the personal data (only for data not obtained directly from the data subject)
* Any recipient or categories of recipients of the personal data
* Detailed information of any transfers to third countries and safeguards in place
* The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
* The right to lodge a complaint with the ICO, and internal complaint procedures
* The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
* Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
* Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

# Subject Access Requests

What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

How we deal with subject access requests

We must provide an individual with a copy of the information the request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the DPO before extending the deadline.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

Data portability requests

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the DPO first.

# Right to erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

* Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
* Where consent is withdrawn
* Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
* The personal data was unlawfully processed or otherwise breached data protection laws
* To comply with a legal obligation
* The processing relates to a child

How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

* To exercise the right of freedom of expression and information
* To comply with a legal obligation for the performance of a public interest task or exercise of official authority
* For public health purposes in the public interest
* For archiving purposes in the public interest, scientific research, historical research or statistical purposes
* The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

* We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
* The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

The right to restrict automated profiling or decision making

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

* It is necessary for the entry into or performance of a contract.
* Based on the individual’s explicit consent.
* Otherwise authorised by law.

In these circumstances, we must:

* Give individuals detailed information about the automated processing.
* Offer simple ways for them to request human intervention or challenge any decision about them.
* Carry out regular checks and user testing to ensure our systems are working as intended.

# Third parties

Using third party controllers and processors

As a data processor, we must have written contracts in place with any third party data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Contracts

Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

* Acting only on written instructions
* Those involved in processing the data are subject to a duty of confidence
* Appropriate measures will be taken to ensure the security of the processing
* Sub-processors will only be engaged with the prior consent of the controller and under a written contract
* The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
* The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
* Delete or return all personal data at the end of the contract
* Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
* Nothing will be done by either the controller or processor to infringe on GDPR.

# Criminal offence data

### Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. You must have approval from the DPO prior to carrying out a criminal record check.

# Audits, monitoring and training

Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must conduct a regular data audit as defined by the DPO and normal procedures.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. CyanGate, LLC will keep this policy under review and amend or change it as required. You must notify the DPO of any breaches of this policy. You must comply with this policy fully and at all times.

Training

You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

If you require additional training on data protection matters, contact the DPO.

# Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. CyanGate, LLC has a legal obligation to report any data breaches to a Lead Supervisory Authority (LSA) within 10 business days.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

* Investigate the failure and take remedial steps if necessary
* Maintain a register of compliance failures
* Notify the LSA of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Please refer to our **Information Security Breach Report** for our reporting procedure.

Failure to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organization at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

1. Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone. [↑](#footnote-ref-1)
2. Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter* *alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements. [↑](#footnote-ref-2)
3. This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision. [↑](#footnote-ref-3)