Data Processing
Privacy Policy

V1

1) Introduction

This Data Processing Privacy Policy sets out how CCTech Ltd (”we”, “our”, “us”, “the Company”) handle the Personal Data of our customers, and those of our clients.

This Data Processing Privacy Policy applies to all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present clients, their customers or website users.

2) Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the Company and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

The DPO is responsible for overseeing this Data Processing Privacy. That post is held by:

Paul Meehan
Data Protection Officer
CCTech Ltd
Unit 2
Olympic Court
Whitehills Business Park
Blackpool
FY4 5GU

Please contact the DPO with any questions about the operation of this Data Processing Privacy Policy or the GDPR or if you have any concerns that this Data Processing Privacy Policy is not being or has not been followed.

3) Personal Data Protection Principles

We adhere to the principles relating to processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Customers for longer than is necessary for the purposes for which the data is processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Customers and Customers are allowed to exercise certain rights in relation to their Personal Data (Customers Rights and Requests).

(i) Made available to clients and Customers and Customers are allowed to exercise certain rights in relation to their Personal Data (Customers Rights and Requests)

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

4) Lawfulness, Fairness, Transparency

4.1 LAWFULNESS AND FAIRNESS

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Customer.

We will only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we process Personal Data fairly and without adversely affecting the Customer, and those of our clients

The GDPR allows processing for specific purposes, some of which are set out below:

(a) the Customer has given his or her Consent;

(b) the Processing is necessary for the performance of a contract with the Customer, or our clients;

(c) to meet our legal compliance obligations;

(d) to protect the Customer's vital interests;

(e) to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Customers. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

4.2 CONSENT

We will only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Customer consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

You are easily able to withdraw Consent to Processing at any time and withdrawal will be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the you first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Categories of Personal Data and Criminal Convictions Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Special Categories of Personal Data and Criminal Convictions Data. Where Explicit Consent is required, we will issue a Privacy Notice to you to capture Explicit Consent.

We will need to evidence Consent captured and will keep records of all Consents in accordance with Related Policies and Privacy Guidelines so that the Company can demonstrate compliance with Consent requirements.

4.3 TRANSPARENCY (NOTIFYING YOU)

The GDPR requires Data Controllers to provide detailed, specific information to you depending on whether the information was collected directly from you or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that you can easily understand them.

Whenever we collect Personal Data directly from you, we must provide you with all the information required by the GDPR including the identity of the Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Customer first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we will provide you with all the information required by the GDPR as soon as possible after collecting/receiving the data. We will also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

5) Purpose Limitation

Personal Data will be collected only for specified, explicit and legitimate purposes. It will not be further Processed in any manner incompatible with those purposes.

We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed you of the new purposes and you have Consented where necessary.

6) Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

We may only process Personal Data when performing our job duties requires it. We cannot Process Personal Data for any reason unrelated to our job duties.

We may only collect Personal Data that we require for our job duties: do not collect excessive data. We ensure any Personal Data collected is adequate and relevant for the intended purposes.

We will ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

7) Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

8) Storage Limitation

Personal Data will not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

We will not keep Personal Data in a form which permits the identification of you for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

We will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

We will ensure that you are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

9) Security Integrity & Confidentiality

9.1 PROTECTING PERSONAL DATA

Personal Data will be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

We are responsible for protecting the Personal Data we hold. We will implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. We will exercise particular care in protecting Special Categories of Personal Criminal Convictions Data from loss and unauthorised access, use or disclosure.

We will follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. We may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

9.3 REPORTING A PERSONAL DATA BREACH

The GDPR requires Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Customer.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify you or any applicable regulator where we are legally required to do so.

10) Transfer Limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. We transfer Personal Data originating in one country across borders when we transmit, send, view or access that data in or to a different country.

We may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Customers' rights and freedoms;
(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
(c) the Customer has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Customer, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Customer where the Customer is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

11) Your Rights & Requests

You have rights when it comes to how we handle your Personal Data. These include rights to:
(a) withdraw Consent to Processing at any time;
(b) receive certain information about the Data Controller's Processing activities;
(c) request access to your Personal Data that we hold;
(d) prevent our use of your Personal Data for direct marketing purposes;
(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
(f) restrict Processing in specific circumstances;
(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
(i) object to decisions based solely on Automated Processing, including profiling (ADM);
(j) prevent Processing that is likely to cause damage or distress to the Customer or anyone else;
(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
(l) make a complaint to the supervisory authority; and
(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

We will verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade us into disclosing Personal Data without proper authorisation).

12) Accountability

12.1 The Controller will implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Company must have adequate resources and controls in place to ensure and to document GDPR compliance including:
(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Customers;
(c) integrating data protection into internal documents including this Data Processing Policy, Related Policies, Privacy Guidelines or Privacy Notices;
(d) regularly training Company Personnel on the GDPR, this Data Processing Privacy Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Customer's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and
(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

12.2 RECORD KEEPING

The GDPR requires us to keep full and accurate records of all our data processing activities.

We will keep and maintain accurate corporate records reflecting our Processing including records of Customers' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Customer types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

12.3 TRAINING AND AUDIT

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

We will undergo all mandatory data privacy related training and ensure our team undergo similar mandatory training.

We will regularly review all the systems and processes under your control to ensure they comply with this Data Processing Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

12.4 PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

We will assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:
(a) the state of the art;
(b) the cost of implementation;
(c) the nature, scope, context and purposes of Processing; and
(d) the risks of varying likelihood and severity for rights and freedoms of Customers posed by the Processing.

Data controllers must also conduct DPIAs in respect to high risk Processing.

We will conduct a DPIA (and discuss our findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:
(e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
(f) Automated Processing including profiling and ADM;
(g) large scale Processing of Special Categories of Personal Data or Criminal Convictions Data Data; and
(h) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:
(i) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
(j) an assessment of the necessity and proportionality of the Processing in relation to its purpose;
(k) an assessment of the risk to individuals; and
(l) the risk mitigation measures in place and demonstration of compliance.

12.5 AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:
(a) a Customer has Explicitly Consented;
(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed but such Special Categories of Personal Data and Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Customers must be informed when we first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Customer's rights and freedoms and legitimate interests.

We must also inform you of the logic involved in the decision making or profiling, the significance and envisaged consequences and give you the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

12.6 DIRECT MARKETING

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Customer's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Customer in an intelligible manner so that it is clearly distinguishable from other information.

A Customer's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

12.7 SHARING PERSONAL DATA

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

We may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

We may only share the Personal Data we hold with third parties, such as our service providers if:
(a) they have a need to know the information for the purposes of providing the contracted services;
(b) sharing the Personal Data complies with the Privacy Notice provided to the Customer and, if required, the Customer's Consent has been obtained;
(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
(d) the transfer complies with any applicable cross border transfer restrictions; and
(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

13) Changes to this Data Processing Privacy Policy

We reserve the right to change this Data Processing Privacy Policy at any time so please check back regularly to obtain the latest copy of this Data Processing Privacy Policy. We last revised this Data Processing Privacy Policy on 04/04/2020.

This Data Processing Privacy Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

14) Definitions

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company name: CCTech Ltd

Company Personnel: all employees, workers contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Customer's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: means personal data relating to criminal convictions and offences.

Customer: a living, identified or identifiable individual about whom we hold Personal Data. Customers may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Customer or information relating to a Customer that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Policy: the Company privacy/GDPR related policy provided to assist in interpreting and implementing this Data Processing Privacy Policy and Related Policies, available on request.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Customers when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Company's policies, operating procedures or processes related to this Data Processing Privacy Policy and designed to protect Personal Data, available on request

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.