UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018.

Full Privacy Policy including working practices, recording procedures.

Mark Crozier for Future Corporate Technologies Limited

Contents:

Section 14……

Appendix , guidance and tables, training records……

Section 1: Business Information

NAME:	**Future Corporate Technologies Limited**
ADDRESS:	**Haverley House Cottage, Seaton Lane, Seaham, SR7 0NQ**
CONTACT NUMBER:	**0191 5359050 and 0191 5130099**
CONTROLLER:	**Mark Crozier**
PROCESSOR:	**Mark Crozier and Callum McHaffie**
ICO REGISTRATION NUMBER:	**ZA823593**
WEBSITE ADDRESS:	**https://futurecorporatetechnologies.co.uk/**
FACEBOOK PAGE:	**https://www.facebook.com/FutureCorporateTechnologies**
TWITTER:	**https://twitter.com/fctservices**
LINKEDIN:	**https://www.linkedin.com/company/future-corporate-technologies-ltd**
EMAIL ADDRESS:	**mark.crozier@fct.services**

Section 1. Business information

Future Corporate Technologies provides businesses with expert, bespoke advice concerning services in both merchant services and business energy. The parent company is an independent sales organisation providing the best offers, advice and savings in partnership with trusted suppliers.

Faster Payment merchant services

Carbon reduction specialists

Section 2. The policy promotes

Adhering to the explicit provisions about documenting processing activities under the UK GDPR

Maintaining records on working processes including processing purposes, data sharing and retention. In line with the demand for small businesses

Maintaining procedures and records of processing activities

Making records available to the ICO if requested

Creates Due diligence and compliance with all aspects of the UK GDPR securing data governance

Controllers and processors documentation obligations awareness

Recording in writing. Update reflecting any changes in processing activities. Maintaining records electronically

Transparent, clear working structures to any client trusted with their personal data.

A clear indication of how much data the business controls, ensuring all data protection practices are legally compliant.

Meets customers' expectations having access to the policy.

Section 3 Articles Covered

Article 30 of the UK GDPR

The name and contact details of the organisation and data controller

Mark Crozier FCT Limited, Haverley House Cottage, Seaton Lane, Seaham, SR7 0NQ.

Lawful processing Article 6 of UK GDPR,:-

Legal basis Legitimate Interest the processing is necessary.

Three-part test

Identify a legitimate interest - we are pursuing a legitimate interest.

The processing is necessary for the business purpose

Balance - the individuals' interests do not override the legitimate interest.

The legal basis and processing are objectively necessary for the stated purpose.

The lawful basis for customer processing provides the right to erasure, the right to portability but no right to object

The nature of the work carried out means it is necessary

More than just useful

Not just standard practice

It is targeted and proportionate way of achieving the purpose of the business, the information cannot be achieved by any other less intrusive means or by processing less data

Article 4 principles of GDPR: - Data Retention Definitions

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.

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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

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 (but see section 6 of the 2018 Act);

Processor means a natural or legal person, public authority, agency or other **body which processes personal data on behalf of the controller.**

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with

domestic law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Third Party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Representative means a natural or legal person established in the United Kingdom who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

Enterprise means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

Article 5 Processing data

Personal data is

Processed lawfully, fairly and in a transparent manner in relation to the data subject

Collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed creating data minimisation

Accurate and, where necessary kept up to date

Kept in a form which permits identification of subjects for no longer than is necessary for the purposes for which it is processed, it may be stored longer if necessary for archiving purposes.

Processed in an appropriate way ensuring security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage

Always accountable

Erased, rectified or destroyed, timely where necessary

Article 6 Lawfulness of processing

Processing is lawful

Data has given consent for one or more specific purposes

Necessary for the performance of a contract to which the data subject is party, or taking steps for them to be entering into a contract

Article 11 allows additional information to be requested prior to any release of information if there is doubt over identity.

Article 12

The controller shall take appropriate measures to provide any information referred to in Article 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in concise, transparent, intelligible and easily accessible form, using clear and plain language.

Facilitate the exercise of data subjects' rights under Art 15 to 22

Exercise data subjects' rights unless not in position to do so

Requests to provide any information under Articles 15 to 22 to the data subject will be provided without due delay and within one month of the receipt of the request

(Flexibility is exercised by a further two months taking into account the complexity and number of requests)

If the request for information is not actioned, the controller must inform the data subject of any necessary extension, and the reasons why. The data subject must be informed of why action has not been taken and their right to lodge a complaint with ICO

Information should not have a fee attached unless it is unfounded or excessive, repetitive there may be –

Reasonable charge

Refuse to act on the request

Need to demonstrate the unreasonableness of the request.

Article 13. Information to be provided where personal data are collected from the data subject

At the time of collecting personal data from the data subject the controller will provide the following information

Identity and contact details of the controller

Purposes for processing and legal basis as set out in the policy

Where applicable the legitimate interests pursued by the controller or by a third party

Fair and transparent processing

Period of time which the personal data will be stored or criteria used to determine that period

Right to access, rectification and erasure of personal data and data portability

Right to withdraw at any time

Information on further processing prior to any further processing taking place

Right to make a complaint to the ICO

Article 14 Right of information where personal data have not been obtained from the data subject

Identity and contact details of the controller

Purposes for processing and legal basis as set out in the policy

Categories of personal data concerned

Recipients of the personal data

The legitimate interests pursued by the controller or a third party

Right to request access rectification or erasure of personal data

Right to withdraw

Right to lodge a complaint

Which source the personal data originated from

Article 15 right of access by the data subject

Article 20 right to data portability

The data subject consents to processing by automated means without prejudice

Article 32 of GDPR

Demonstrating technical and organisational measures implemented to protect the personal data stored. Include ways data is stored and protected, preventing data breaches, physical and or technical incidents

Section 4 Necessity of Processing

Assessed and implemented in accordance with the principles underpinning the Regulation which are:

Fairly and lawfully processed

Processed for limited purposes

Adequate relevant and not excessive

Accurate

Not kept for longer than is necessary

Processed in line with your rights

Secure

Section 5 Lawful Basis for processing

Legitimate interests. The process is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individuals personal data which overrides those legitimate interests

Legitimate interests has been identified as the appropriate lawful basis taking into consideration

Who does the process benefit? – **customers, third party providers**

Would individuals expect this processing to take place? **yes**

What is the relationship with the individuals? - **customers and prospective / future customers**

Are you in a position of power over them? **no**

What is the impact of the processing on the individual? **none on a normal basis may have data capture used if there is a requirement legally**

Are they vulnerable? **no**

Are some of the individuals concerned likely to object? **no**

Are you able to stop the processing at any time on request? **Yes**

Section 6: Accountability

Legal requirement for data sharing we will ensure -

Staff are adequately trained.

Data processing is assessed regularly

Risk and data protection impact assessments

Measures are in place to ensure compliance and no breach of data protocols

Conducting data protection impact assessment for high-risk processing

Data protection is part of the day-to-day processes of our environment

Records kept updated and secured

Legal basis identified

Record management and security

Duty of confidence when we process information

Section 7 Additional Legislation

Industry governing bodies

Section 8: Procedures, Protocols and working practices

Purchase of leads

https://www.marketscan.co.uk/

Data is purchased by paying for a specific number leads which include contact number, name and email address.

We work with the third party firm Marketscan who request payment, prior to the purchase which is allocated as a credit onto our business online portal under the account of Future Corporate Technologies Limited.

This is a secure bespoke portal allocated by the third party provider. Access is strictly by user name and password.

Access to the portal is by trained and authorised staff only. Records of log on are available.

The third party leads are GDPR compliant with no data supplied including any individual registered with TPS warnings. The lead provider monitors use of the leads in terms of times used, any complaints etc.

The data purchased expires after 12 months.

Within the data purchase agreement if there were to be any rogue data which resulted in a complaint, the data provider be referred back to Marketscan with the corresponding reference number liability being theirs. Recommendation of referral to the ICO.

Markertscan are currently the sole business we work with purchasing leads.

We hold a comprehensive CRM which has been formulated through previous customer data, referrals, networking and referrals from existing customers. Also new leads through employees who have agreed to deal with us.

This data is used for both Future Corporate Technologies Limited providing corporate energy efficient contracts.

Data protection agreement with third parties

Our service providers, energy suppliers and partners, supply Third Party agreements TPI including privacy, confidentiality and data protection statement.

Hard copies are filed in Teams folders.

NDA agreements prior to any communication regarding customers' data with potential partners.

Sellers, staff, agents and employees commit to appropriate training, this is documented and recorded in training manual, data protection contracts are signed will all.

Storage of information and downloaded documents

Company documents are stored in Teams with restricted password.

Individual customer information is received by email, Watsapp or on-line application forms which are through Jot Form on the company website. It is recommended where possible information should be sent as an encrypted file.

We have a bespoke CRM system, the information and documentation we receive from the customer is uploaded onto their own individual allocated file. Documents are then securely destroyed or deleted.

CRM is only accessible to relevant staff, agents, directors and admin. CRM enables remote access to the secured system by mobile phone, which provides immediate security to the data. All data is fully deleted from the mobile device. Any photographic data storage is deleted from the devices hard drive.

There are no customer files stored anywhere outside of the CRM.

Online query/ application form through Jotform customer data is stored which is html integrated into website.

Docusign - There are two accounts used
Powwr Portal
Future Corporate Technologies Limited own Docusign. This stores all leads and contracts accessed through email of info@fct.services
Limited access to agents or employees who are aware fully of the Data Protection importance and procedures all of whom have signed Privacy Notices.

Social media is used:-

Linkedin
Facebook
Instagram
Twitter

Usage is secured and limited to agents or employees who are aware fully of the Data Protection importance and procedures all of whom have signed Privacy Notices.

The same procedure as mobile phone usage is practiced once the data has been retrieved.

External Third-party requirements for card services

Customer files, ID and proofs are submitted to V9, technology and payment experts via their bespoke online portal, which is password protected.

Customer files, ID and proofs are submitted to UTP Merchant Services Ltd, specialists in providing credit card machines to businesses via their bespoke online portal, which is password protected.

Customer files, ID and proofs are submitted to Chip and Pin Direct, specialists in card payment providers with a 5-star customer service through their bespoke online portal, which is password protected.

External Third-party requirements for Energy Suppliers

All information required by energy suppliers are submitted via their own secure portals. There are 35 suppliers for use including Powrr, each having their own secure individual portals.

Mark Crozier Sole Director has access to all customer data, via laptop as well as remote hard drive.

Mark is the sole person having full access to this data.

Mobile phone usage / workplace tool

Information received or stored on mobile phones, which is an effective way of working within the business is uploaded daily.

Staff has been trained to follow out this procedure and are aware of data protection responsibilities.

Telephone calls

Telephone calls are recorded through the telephone system ring central, customers are informed they are being recorded, all recordings are uploaded into the secure cloud system or onto the ring central portal system, which is secured by log in and password.

Access to this information is by Director level only.

Storage of information and destruction/deletion of expired information

CRM, customer portals and secure teams' files. All documents are allocated to the correct system all information is digital.

Any hard copy documents are scanned into secure folders, transferred to the correct system, the hard copy is then securely destroyed by shredding which is securely disposed of.

Paper copies are irregular as all business matters are dealt with electronically.

There is a number of filing cabinets in the office where relevant hard paperwork is stored, these are all fitted with a lock and key system, all paperwork is secured daily, staff operate clear desk policy leaving no data exposed.

Time limits of keeping data

Data is kept indefinitely on the CRM system, which is a licensed, charged bespoke system. The time the data is retained is defined by the provision of the service.

Portal access is jointly agreed with the third parties, again the duration of the data depends on the services and the customers permission.

Access is granted as long as we are working in partnership with the third-party providers. Time limits can be flexible as contracts may be rolling for an extended period of time.

Where customers request their data be removed, it is actioned as soon as possible.

Summary of where data is stored

Data stored:

CRM

FCT Teams folder

Ring central phone system and portal

Supplier Portals

Powwr Portal

V9, UW and UTP individual portals

Service Providers Portals 35 in total

UW portal and data is accessible to MC and CM only

Go Daddy website and email marketing campaigns accessed only by authorised administration staff, agreements are in place when working on marketing which fully cover the demands and responsibilities of the company under the relevant Data Protection laws.

Outlook/Professional business e mails are through Go Daddy

Locked filing cabinets

Website provides cookies and tracking all linked to Go Daddy website

No Crm System - Cloud Based used via phone and laptop and pc - it is secure

Laptops and pc's secured with security software and passwords

Security software

Storage of data and emergency back up

There is a 1 mwh remote hard drive , this is secured by the company director

Sensitive data is saved on the hard drive, only in secured cloud software

Email and website backups are securely in place with go daddy.com

CCTV in the workplace

One of the most intrusive forms of data collection

CCTV is part of the working system within the office, providing further security for employees and agents, as well as lone workers

The CCTV is identified by appropriate signage. The company director is the controller, indicated on the appropriate signage

The use of CCTV is appropriate and not used intrusively. There are the appropriate number of cameras adding another layer of protection to the systems within the office

The system is fully protected by log in and password with access being restricted to the director.

Remote access is available to the director, this will be accessed for security, safety and working purposes only

Information reflecting the above is available to anyone entering the office area.

The controller is the only person who can access and downloaded footage.

The system is in a safe environment with access controlled strictly by password.

Documentation of the download footage including the reason for it being necessary, the time, date duration of footage captured will be recorded in a log attached to this policy.

Any third party who requests and then receives any data captured will be fully documented in the log with them signing the log for audit purposes.

A copy of the ICO is in the picture. A data protection code for practice for surveillance cameras and personal information is available at ICO.org.uk.

Guide to UK GDPR is available at ICO.org.uk

Section 9: Responsibilities

There has been a review of the purposes of the processing activities and as a result the most appropriate lawful basis has been chosen for the activity

Processing is necessary for the relevant purpose, accepting that there is no other reasonable way to achieve that purpose

There is documentation reflecting the decision on which lawful basis applies to help us demonstrate compliance

The Privacy notice includes information about both the purposes of the processing and lawful basis for the processing

Transferring data for the purposes of third-party usage are documented and recorded

Section 10 Reporting a breach

Article 19:

Not every breach needs to be reported however if a security breach has a significant impact, you MUST notify the ICO within 72 hours

You must notify your users if they are likely to be affected

Consider whether to inform anyone else who might be affected

If you are unsure whether any of the above applies it is safer to report the breach to the ICO

If your breach is likely to adversely affect any users or customers, you will also need to advise them of the breach without undue delay

You can choose how to inform them as long as it is done and reaches them promptly what should be included is:

Your name and contact details

The date of the breach

A summary of the incident

The likely effect on them

Any measures you have taken to address the breach and

Any steps they can take to protect themselves from harm

You should take into consideration if any other persons need to be informed of the breach say any end users relying on the integrity or trust of the service

The ICO will give advice if the breach needs to be informed publicly. This will only occur if it is in the interest of the public.

Future Corporate Technologies Limited is registered with the ICO as a company storing data if there were to be any breaches.

A confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorised fashion. This could be for the following reasons:

Personal Health Information (PHI)

Personally Identifiable Information (PII)

Trade secrets

Intellectual property

A security incident in which sensitive protected or confidential data is copied transmitted viewed stolen or used by an individual unauthorised to do so usually involving vulnerable unstructured data files documents and sensitive information

Section 11 Record management

Future Corporate Technologies Limited recognises that it is vital that we manage records as it is to deliver the service in an orderly efficient and accountable manner

In doing so we ensure that records in all formats are accurate, reliable, ordered, complete useful, up to date and accessible whenever it is needed

Our aim in using effective management includes -

Help us carry out our business

Protect the rights of all individuals

Ensure regulation compliance

Provide an audit trail to meet all requirements

Support continuity and consistency

Ensure openness transparency and fairness

Section 12 Individuals working responsibilities within the business.

Everyone has their individual roles and responsibilities to ensure the details are appropriately managed

Directors and staff, agents and third parties are ensuring the smooth running of the organisation, demonstrating the day to day working policies and procedures are carried out daily.

Anyone who receives, creates, maintains or has access to any of the company documents or records is responsible for ensuring that they act in accordance with records management stipulation and procedures. Induction and intermittent training is provided with records being available.

Section 13 Recommendations

Always maintain the ICO registration it is easy to become registered simply visit ico.org.uk you can register on an annual basis paying by direct debit (this saves you £5 and means you do not need to re-register as the payment is taken out annually)

Audit for all records needs to be maintained

Training needs to be carried out with an audit maintained

Processes recorded

CCTV signs need to be sited and include the following information -

CCTV is being recorded at all times.

Name of the processor if anyone wants to contact them to discuss any data capture

Telephone number for anyone to contact the processor

Noncompliance with signs and details could result in a breach.

CCTV remote access it is recommended that anyone with mobile footage access by tablet phone or other means have an extra measure of securing the data in place. In the event of the loss of equipment it should be documented in the policy how extra security to secure such data is taken.

There are several apps for smart phones which allow apps to be deleted it is recommended as well as having password protection these steps are taken to demonstrate complete due diligence.

Privacy policy needs to be always available to all persons.

It is recommended that consideration is given to the needs of the business on an annual basis, this would lead to an assessment about the legal basis of processing.

Section 14 APPENDIX:

1. Data Authority Register
2. https://www.marketscan.co.uk/insights/5-steps-to-maintaining-a-gdpr-compliant-database-

Name	Date	Time	Reason for data	Training, breach, incident	Details for compliance