Eco Efficient Home Solutions Ltd t/as EEH Solutions Integrated Management System		
Document Title:	**General Data Protection Regulation Policy and Procedure**	
Ref. No.:	**GDPP012**	
Document Users / Security Class:	**All Users**	
Next Review Date	**One Year**	

Foreword: General Data Protection Regulation (UK GDPR)

Passed by the European Union in April of 2016, the GDPR had far reaching global impact on data security. No matter where you were based, any organisation that did business with EU citizens had to comply with the GDPR's expanded and more stringent data protection rules by **May 25th, 2018.**

The UK voted to leave the EU in 2016 and officially left the trading bloc – it's nearest and biggest trading partner – on 31st January 2020. However, both sides agreed to keep many things the same until 31st December 2020, to allow enough time to agree to the terms of a new trade deal.

The GDPR was an EU Regulation and from the 1st January 2021 no longer applies to the UK. However, our organisation operates inside the UK, and so we will need to comply with UK data protection law. The GDPR has been incorporated into UK data protection law as the UK GDPR – so in practice there is little change to the core data protection principles, rights and obligations found in the EU GDPR. The EU GDPR is an EU Regulation and it no longer applies to the UK. We operate inside the UK, and need to comply with the Data Protection Act 2018 (DPA 2018).

On 28th June 2021, the EU approved adequacy decision for the EU GDPR and the Law Enforcement Directive (LED). This means data can continue to flow as it did before, in the majority of circumstances. Both decisions are expected to last until 27th June 2025. Most EEA processors will be able to send personal data back to UK controllers with no restrictions.

The EU GDPR may also still apply directly if we operate in the European Economic Area (EEA), offer goods or services to individuals in the EEA, or monitor the behaviour of individuals in the EEA.

The ICO will not be the regulator for any European-specific activities caught by the EU version of the GDPR, although they hope to continue working closely with European supervisory authorities.

The Data Protection Act 2018 (DPA 2018) continues to apply. The provisions of the EU GDPR were incorporated directly into UK law at the end of the transition period. The UK GDPR sits alongside the DPA 2018 with some technical amendments so that it works in a UK-only context.

The ICO will remain the independent supervisory body regarding the UK's data protection legislation.

The UK government will continue to work towards maintaining close working relationships between the ICO and other countries' supervisory authorities once the transition period ends.

The principles of the EU GDPR have been incorporated in UK Data Protection law, so we will continue to use our existing policies and procedures. We have updated this policy and procedure to reflect that the Brexit transition period has ended. We will continue to keep our policies under review and update it where necessary.

The Guide to the UK GDPR is part of the ICO's Guide to Data Protection. It is for DPOs and others who have day-to-day responsibility for data protection. It explains the general data protection regime that applies to most UK businesses and organisations. It covers the UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018.

It explains each of the data protection principles, rights and obligations and summarises the key points which are contained in this policy and procedure.

Where relevant, this guide also links to more detailed guidance and other resources, including ICO guidance and statutory ICO codes of practice. Links to relevant guidance published by the European Data Protection Board (EDPB) are also included for reference purposes.

This GDPR Policy and Procedure is to be read in conjunction with our Data Retention and Disposal Policy.

1. POLICY STATEMENT

The UK GDPR sets out 7 key principles.

Lawfulness, fairness and transparency
Purpose Limitation
Data minimisation
Accuracy
Storage Limitation
Integrity and Confidentiality (security)
Accountability principle

Our company needs to collect personal information about the people we deal with to effectively and compliantly carry out our everyday business functions and activities and to provide the products and services defined by our business type. This information can include

(but is not limited to), name, address, email address, data of birth, IP address, identification number, private and confidential information, sensitive information and bank details.
In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the UK General Data Protection Regulation and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

Our company has developed policies, procedures, controls and measures to ensure continued compliance with the UK GDPR and its principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and safety of personal and/or special category data belonging to the individuals with whom we deal is paramount to our company ethos and adheres to the UK GDPR and its associated principles in every process and function.

> ***We are proud to operate a 'Privacy by Design' approach and aim to be proactive not reactive; assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.***

2. PURPOSE

The purpose of this policy is to ensure that our organisation is meeting its legal, statutory and regulatory requirements under the UK GDPR and to ensure that all personal and special category information is safe, secure and processed compliantly whilst in use and/or being stored and shared by us. We are dedicated to compliance with the UK GDPR's principles and understand the importance of making personal data safe within our business.

To this end, we provide our staff with regular training sessions, including access to on-line e-learning courses and quizzes, compliance updates and assessments regarding the UK GDPR rules, principles and guidelines to ensure their knowledge and understanding of this area is adequate, effective and relevant to their role. The measures in this policy are compliant with the UK GDPR rules and as such, support our staff and give them the confidence and competence to process personal information compliantly.

The UK GDPR includes provisions that promote accountability and governance and as such our firm has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data.

3. SCOPE

The policy relates to all staff *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, and agents engaged with our organisation in the UK or overseas)* within the organisation and has been created to ensure that staff deal with the area that this policy relates to in accordance with legal, regulatory, contractual and business expectations and requirements.

Transfers of data from the UK to the European Economic Area (EEA) are not restricted. The EU has agreed to delay transfer restrictions from the EEA to the UK (known as the bridge). This enables personal data to flow freely from the EEA to the UK until either adequacy decisions are adopted, or the bridge ends.

Unless the EU Commission makes an adequacy decision before the bridge ends, EU GDPR transfer rules will apply to any data coming from the EEA into the UK. We therefore need to consider what safeguards we can put in place to ensure that data can continue to flow into the UK if required, which is unlikely.

4. 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.

• **Data** subject means an individual who is the subject of personal data

• **Data Controlle**r 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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

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

• **Third Party** means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

• **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.

• **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 Union or Member State 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.

• **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.

• **Genetic Data** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

• **Biometric Data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

• **Cross Border Processing** means processing of personal data which: -

- takes place in more than one Member State; or
- which substantially affects or is likely to affect data subjects in more than one Member State

• **Representative** means a natural or legal person established in the EU who, designated by the controller or processor in writing represents the controller or processor with regard to their respective obligations under this Regulation.

• **Supervisory Authority** means an independent public authority which is established by a Member State

• **Binding Corporate Rules** means personal data protection policies which are adhered to by our organisation for transfers of personal data to a controller or processor in one or more third countries or to an international organisation

5. DATA PROTECTION REGULATION BACKGROUND

The UK initially had The Data Protection Act 1984 in place to regulate the use of processed information that related to individuals. However, in 1995 the introduction of EU Directive 95/46/EC which set aims and requirements for member states on the protection of personal data when processing or sharing, meant an updated Act was required.

The UK subsequently developed and enacted The Data Protection Act 1998 (DPA) to ensure that British law complied with the EU Directive and to provide those with obligations under the Act, with updated rules, requirements and guidelines for processing and sharing personal data.

2018 marked the 20th anniversary of the DPA enactment and whilst there have been periodical additions or alterations to the Act, technology has advanced at a far faster rate, necessitating new regulations for the current digital age. The past 20 years has also seen a vast increase in the number of businesses and services operating across borders, further highlighting the international inconsistency in Member States individual data protection laws.

For this reason, in January 2012, the European Commission proposed a new regulation applying to all EU Member States and bringing a standardised and consistent approach to the processing and sharing of personal information across the EU. The UK was then an EU member state so the provisions of GDPR applied to our company.

The Data Protection Act 2018 (DPA 2018) continues to apply. The provisions of the EU GDPR were incorporated directly into UK law at the end of the Brexit transition period. The UK GDPR sits alongside the DPA 2018 with some technical amendments so that it works in a UK-only context.

6. UK GENERAL DATA PROTECTION REGULATION (GDPR)

The Data Protection Act 2018 controls how personal information is used by organisations, businesses or the government.

As our organisation processes personal information regarding individuals (*data subjects*), we are obligated under the UK General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with the UK GDPR and its principles.
Information protected under the UK GDPR is known as "personal data" and is defined as: -

> ***"Any information relating to an identified or identifiable natural person; 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."***

We ensure that even greater care and attention is given to personal data falling within the UK GDPR's 'special categories' (previously referred to under the DPA as sensitive personal data), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the 'Special categories of Personal Data' the UK GDPR advises that: -

> ***Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.***

The UK GDPR regulates the processing of personal data, which includes organisation, altering, adapting, retrieving, consulting on, storing, using, disclosing, transmitting, disseminating or destroying any such data. As our organisation uses personal data in one or more of the above capacities, we have put into place robust measures, policies, procedures and controls concerning all aspects of personal data handling.

6.1 THE UK GDPR PRINCIPLES

The UK GDPR requires that personal data shall be: -

a) Processed lawfully, fairly and in a transparent manner in relation to individuals

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

The controller shall be responsible for, and be able to demonstrate, compliance with the principles and requires that firms show how they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

6.2 THE INFORMATION COMMISSIONERS' OFFICE (ICO)

The Information Commissioners Office (ICO) is an independent regulatory office who report directly to Parliament and whose role it is to uphold information rights in the public interest. The legislation they have oversight for includes: -

- The Data Protection Act 1998 (pre-25th May 2018)
- The UK General Data Protection Regulations (post-1st January 2021)
- The Data Protection Act 2018
- The Privacy and Electronic Communication (EU Directive) Regulations 2003
- Freedom of Information Act 2000

- The Environmental Information Regulations 2004

ICO's mission statement is "to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals" and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

The ICO will remain the independent supervisory body regarding the UK's data protection legislation.

The UK government will continue to work towards maintaining close working relationships between the ICO and other countries' supervisory authorities once the transition period ends.

Our organisation is registered with ICO and appears on the Data Protection Register as a processor of personal information.

7. OBJECTIVES

We are committed to ensuring that all personal data obtained and processed by our organisation is done so in accordance with the UK GDPR and its principles, along with any associated regulations and/or codes of conduct laid out by the Supervisory Authority and local law. We are dedicated to ensuring the safe, secure, ethical and transparent use of all personal data and to uphold the highest standards of data processing.

We use the objectives below to meet the regulatory requirements of the UK GDPR and to develop measures, procedures and controls for maintaining and ensuring compliance.

We ensure that: -

- We protect the rights of individuals with regards to the personal information known and held about them by our organisation in the course of our business.
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the UK GDPR.
- We spot check that the process is carried out by our organisation and is monitored for compliance with the UK GDPR and its principles.
- Data is only obtained, processed or stored when we have met the lawfulness of processing requirements
- We record consent at the time it is obtained and can evidence such consent if required.
- All employees (including new starters and agents) are competent and knowledgeable about their UK GDPR obligations and are provided with training in

the UK GDPR principles, regulations and how they apply to our business and services.

• Customers feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the UK GDPR.

• We maintain a continuous program of monitoring, review and improvement with regards to compliance with the UK GDPR and to identify gaps and non-compliance before they become a risk.

• We monitor the Latest News from the ICO email, to stay abreast of updates, notifications and additional requirements.

• We have robust and recorded Complaint Handling and Breach Incident controls and procedures in place for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection.

• We have appointed a member of staff who takes responsibility for the overall supervision and implementation of the UK GDPR and its principles and remains informed on the regulations and how they relate to our organisation.

• We will put an Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program utilises this policy and procedure and the UK GDPR itself to ensure continued compliance.

• We provide clear lines of reporting and supervision with regards to data protection compliance.

• Develop and maintain strict and robust DPA procedures, controls and measures to ensure continued compliance with the Act.

• We store and destroy all personal information, in accordance with the UK GDPR timeframes and requirements and in line with our Data Retention and Disposal Policy.

• Any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

8. DATA PROTECTION OFFICER

A Data Protection Officer (DPO) must be appointed by a firm where: -

• The processing is carried out by a public authority or body (except for courts acting in their judicial capacity)

• the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale

• the core activities of the controller/processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

We have appointed a DPO and have allocated DPO responsibilities to an internal Compliance Manager who will be supported by external specialists.

GOVERNANCE PROCEDURES

9. ACCOUNTABILITY & COMPLIANCE

Due to the nature, scope, context and purposes of processing undertaken by our organisation we will carry out risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have also implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the UK GDPR and any codes of conduct under which we have obligations.

We can demonstrate that all processing activities are performed in accordance with the UK GDPR and that we have in place robust policies, procedures, measures and controls for the protection of data. We operate a transparent workplace and work diligently to guarantee and promote a comprehensive and proportionate governance program.

We operate a top-down approach to data protection and ensure that every employee within the company is knowledgeable about and has access to the UK GDPR requirements, its principles, related codes of conduct and out internal policies, measures and training documents. Staff will be tested periodically to assess their level competency and understanding of the data protection regulations and to demonstrate our commitment to protecting the information that we process.

Our main governance objectives are to: -

• Educate senior management and employees about the requirements under the UK GDPR and the possible impact of non-compliance
• Provide a dedicated and effective data protection training program for all staff
• Identify key senior stakeholders to support the data protection compliance program
• Allocate responsibility for data protection compliance and ensure that the designated person has sufficient access, support and budget to perform the role
• Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organisational measures that our organisation has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated policies (e.g. Training Policy, Audit Procedures etc). These measures include: -

- GDPR Policy & Procedure
- Staff Training & Development Policy
- Internal Audits & Monitoring Policy & Procedures
- Clear Desk Policy
- Appointed person responsible for Data Protection
- Business Continuity Plan & Daily Data Backups

9.1 PRIVACY BY DESIGN

We operate a 'Privacy by Design' approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We therefore have additional measures in place to adhere to this ethos, including: -

Data Minimisation

One of the UK GDPR, principles advises that data should be *'limited to what is necessary'*, which forms the basis of our minimal approach. We only ever obtain, retain, process and share the data that is essential to carry out our services and legal obligations and we only keep if for as long as is necessary, usually for 6 years.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the UK GDPR.

Measures to ensure that only the necessary data is collected includes: -

- Electronic collection (i.e. forms, website, surveys etc) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include 'optional' fields, as optional denotes that it is not necessary to obtain
- Physical collection (i.e. face-to-face, telephone etc) is supported using scripts and internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected
- We have SLA's and bespoke agreements in place with third-party controllers who send us personal information (either in our capacity as a controller or processor). These state that only relevant and necessary data is to be provided as it relates to the processing activity we are carrying out.

• We have documented destruction procedures in place where a data subject or third-party provides us with personal information that is surplus to requirement as outlined in our separate Data Retention and Disposal Policy.

Encryption

Encryption may sometimes be used where a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key, although this is not common throughout our organisation or considered a necessity.

Restriction

Our Privacy by Design approach means that we use company-wide restriction methods for all personal data activities. Restricting access is built into the foundation of our organisations processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information.

Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options (i.e. contracts, permissions, personal records). Where this is necessary, we utilise a tiered approach to minimise the information we hold and/or the length of time we hold it for.

Steps include: -

• In the first instance, we always ask the initial data controller to send copies of any personal information records directly to the data subject
• Where step 1 is not possible or feasible, we will obtain a copy of the data and if applicable redact to ensure that only the relevant information remains (i.e. when the data is being passed to a third-party for processing and not directly to the data subject)
• When only mandatory information is visible on the hard copy data, we utilise electronic formats to send the information to the recipient to ensure that encryption methods can be applied (i.e. we do not use the postal system as this can be intercepted).
• Recipients (i.e. the data subject, third-party processer) are reverified and their identity and contact details checked
• The member of staff who takes responsibilities authorises the transfer and checks the file(s) attached and encryption method and key

• Once confirmation has been obtained that the recipient has received the personal information, where possible (within the legal guidelines and rules of the UK GDPR), we destroy the hard copy data and delete the sent message
• If for any reason a copy of the paper data must be retained by our organisation, we use a physical locked cabinet to store such documents

9.2 RESTRICTED ACCESS & CLEAR DESK POLICY

Our organisation may on occasions and at its discretion, place all or part of its files onto a secure computer network with restricted access to all/some personnel data. When implemented, access to personal information will only be granted to the person/department that has a specific and legitimate purpose for accessing and using such information.
Our organisation operates a zero-tolerance Clear Desk Policy and does not permit personal data to be left unattended on desks or in meeting rooms, or in visible formats, such as unlocked computer screens or on fax machines, printers etc. Access to areas where personal information is stored (both electronic and physical) are on a restricted access basis with secure controlled access functions throughout the building. Only staff authorised to access data or secure areas are able to do so. All personal and confidential information in hard copy is stored safely and securely.

9.3 INFORMATION AUDITS

To enable our organisation to comply with the UK GDPR, we will carry out a company-wide data protection information audit to better enable us to record, categorise and protect the personal data that we hold and process.

The audit will identify, categorise and record all personal information obtained, processed and shared by our company in our capacity as a controller which includes: -

• What personal data we hold
• Where it came from
• Who we share it with
• Legal basis for processing it
• What format(s) is it in
• Who is responsible for it?
• Access level (i.e. full, partial, restricted etc)

9.4 PROCESSING CONDITIONS AND ACTIVITIES

At the core of all personal information processing activities undertaken by our organisation, is the assurance and verification that we are complying with the UK GDPR and our lawfulness of processing obligations. Prior to carrying out any processing activity on personal

information, we always identify and establish the legal basis for doing so and verify these with the regulations.

This legal basis is documented on our information audits and is also provided to the data subject and Supervisory Authority under our information disclosure obligations as outlined in this document. Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: -

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which we are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in our organisation
- Processing is necessary for the purposes of the legitimate interests pursued by our organisation or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).

We will monitor any legislation that alters or adds to these conditions and update this document accordingly.

As an organisation with less than 250 employees at the time of constructing this Policy, our organisation maintains records of all processing activities where: -

- Processing personal data could result in a risk to the rights and freedoms of individual
- The processing is not occasional
- We process special categories of data or criminal convictions and offences
- Such records are maintained in writing, are provided in a clear and easy to read format and are readily available to the Supervisory Authority upon request.

9.5 CODES OF CONDUCT & CERTIFICATION MECHANISMS

Our organisation will adhere to any data protection codes of conduct to demonstrate that we comply with the UK GDPR rules and principles. These codes and certification mechanism are approved by the Supervisory Authority and have been disseminated throughout the company to ensure competency and compliance from all staff.

The codes of conduct that we adhere to help us to: -

- Improve transparency and accountability
- Demonstrate to the public and Supervisory Authority that we meet the requirements of the data protection law and that we can be trusted with personal data
- Mitigate against enforcement action(s)
- Improve standards by establishing best practice
- Carry out fair and transparent processing
- Ensure appropriate safeguards within the framework of personal data transfers to third countries or international organisations

We submit to frequent and unscheduled monitoring and audits.

9.6 THIRD-PARTY PROCESSORS

Where our organisation utilises external processors for the personal data that we hold such as:

- IT Systems and Services
- Legal Services
- Debt Collection Services
- Human Resources
- Credit Reference Agencies
- Direct Marketing Services

We have strict due diligence and ***Know Your Customer*** procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain company documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for as outlined in Data Retention and Disposal Policy.

We audit their processes and activities prior to contract and during the contract period to ensure compliance with the data protection regulations and review any codes of conduct that they are obligated under to confirm compliance. The continued protection of the rights of the data subjects is our first priority when choosing a processor and we understand the importance of outsourcing processing activities as well as our continued obligations under the UK GDPR even when a process is handled by a third-party.

We draft bespoke Service Level Agreements (SLAs) and contracts with each processor and among other details, outlines: -

- The processors data protection obligations
- Our expectations, rights and obligations

- The processing duration, aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

That contract or other legal act shall stipulate, in particular, that the processor: -

- Processes the personal data only on our documented instructions
- Seeks our authorisation to transfer personal data to a third country or an international organisation (unless required to do so by a law to which the processor is subject)
- Shall inform us of any such legal requirement to transfer data before processing
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Takes all measures to security the personal data at all times
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights
- Assists our organisation in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments
- When requested, deletes or returns all personal data to our organisation after the end of the provision of services relating to processing, and deletes existing copies where possible
- Makes available to our organisation all information necessary to demonstrate compliance with the obligations set out here and in the contract
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract
- Informs our organisation immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

9.7 RECORDS RETENTION & DISPOSAL

Our organisation has defined procedures for adhering to the retention periods as set out by the relevant legislation and adhere to the UK GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that

protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and priorities the protection of the personal data at all times. Further details are contained in our DPA Retention Policy.

10. PRIVACY IMPACT ASSESSMENTS (PIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected at all times whilst their data is being stored and processed by our organisation. We therefore utilise several measures and tools to reduce risks and breaches for general processing, however when the processing is likely to be high risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where our organisation must or are considering carrying out processing that utilises new technologies, where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we will carry out a Privacy Impact Assessments (PIA) (also referred to as a Data Protection Impact Assessment).

We consider processing that is likely to result in a high risk to include: -

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person(s)
- Processing on a large scale of special categories of data
- Processing on a large scale of personal data relating to criminal convictions and offences
- Systematic monitoring of a publicly accessible area on a large scale (i.e. CCTV)
- Where a processing operation is likely to result in a high risk to the rights and freedoms of an individual
- Those involving the use of new technologies
- New processing activities not previously used
- Processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects
- Processing activities making it difficult for the data subject(s) to exercise their rights

Carrying out PIAs will enable us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach and allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

The PIA enables us to identify possible privacy solutions and mitigating actions to address the risks and protection the privacy and impact. Solutions and suggestions are set out in the PIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either: -

- Eliminated
- Reduced
- Accepted

10.1 PRIVACY IMPACT ASSESSMENT PROCESS (PIA)

A lead is always appointed to carry out the PIA, follow the process, record the necessary information and report the results to the Senior Management Team. All PIAs are carried out in conjunction with the Data Protection Officer or member of staff who takes this responsibility who provides advice and support for the compliance of the processes with the UK GDPR rules.

The PIA lead ascertains if an assessment is required by assessing the answers to the below questions. Where one or more questions result in a 'yes' answer, the assessment is carried out.
Screening questions are: -

- Does the processing require systematic and/or extensive evaluation (via automated means) of personal aspects an individual(s)?
- Will decisions be based on such evaluations that are likely to produce legal effects concerning the individual(s)?
- Is the processing on a large scale and involves special categories of data?
- Is the processing on a large scale and involves data relating to criminal convictions and offences?
- Does the processing involve systematic monitoring of a publicly accessible area on a large scale? (i.e. CCTV)
- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Is the information about individuals likely to raise high risk privacy concerns or expectations?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information or a third-party without adequate safeguards in place?

• Does the processing involve the use of new technology or systems which might be perceived as being privacy intrusive?
• Could the processing result in decisions being made or action being taking against individual(s), in ways that could have a significant impact on them?
• Will the project require you to contact individuals in ways which they may find intrusive?

The PIA is carried out using our predefined document and each stage is recorded to demonstrate compliance and to show that all high-risk processing activities have been assessed prior to being operational. PIAs are retained for 6 years from the date they were first carried out and are readily available for the Supervisory Authority upon request.

The PIA includes: -

1. The aims and objectives of the PIA
2. The scope of the PIA (if covering more than one processing activity)
3. Clarify the legal basis for processing
4. Which activity/high risk reason is the PIA required for (i.e. which of the initial screening questions above have been identified)
5. A description of the processing operations
6. The purpose(s) of the processing and where applicable, the legitimate interests pursued by the controller
7. An assessment of the necessity and proportionality of the processing in relation to the purpose
8. An assessment of the risks to individuals (including possible intrusions on privacy where appropriate)
9. Assess the corporate risks (including regulatory action, non-compliance, reputational damage, loss of public trust etc)
10. Conduct a compliance check against the UK GDPR, relevant legislation and any Codes of Conduct
11. Maintain a record of the identified risks
12. Where appropriate, we seek the views of data subject(s) or their representatives on the intended processing
13. The measures in place to address, reduce or remove the risk (i.e. security, proposed solutions, mitigating actions etc)
14. Data flow – what the information is, where it is coming from, who it is going to
15. Authorisation from the DPO and sign off by Senior Management
16. Record all PIA outcomes & add risk rating & next action

After the assessment questions have been addressed, internal and external consultations are held with employees, agents or third-parties who have a valid input of the processing

activity to ensure that no risks go unmitigated. The Data Protection Officer and IT department are key contributors in the consultation stage, alongside colleagues who play an important part in the actual processing activity and/or protection of data.

The consultation can include: -

- Formal and informal discussions
- Emails and/or letters
- Employee, management & stakeholder meetings
- Board input and approval

After consultations, the processing activity is given a risk rating using the below 'Red, Amber, Green (RAG)' risk matrix. RAG ratings are generated using the likelihood vs impact scores.

LIKELIHOOD	IMPACT					
		Trivial (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
	Almost Certain (5)	Low Med	Medium	High	Very High	Very High
	Likely (4)	Low	Low Med	Med High	High	Very High
	Possible (3)	Low	Low Med	Medium	Med High	High
	Unlikely (2)	Low	Low Med	Low Med	Medium	Med High
	Rare (1)	Low	Low	Low Med	Medium	Medium
Impact Score x Likelihood Score = Risk Rating						

• **GREEN** - Where an assessment outcome is Green, you should see if there are still any solutions or mitigating actions that can be applied to reduce the risk impact down as far as possible. However, most green rated risks are acceptable and so focus should be placed on those with higher ratings. Even where a green RAG rating has been given at the risk/privacy identification stage, this risk should still be added to the mitigating actions template for continuity and to ensure that all risks have been recorded and assessed.

• **AMBER** - Where an assessment outcome is Amber, mitigating action must proposed and applied before processing can be approved. The aim is to reduce all risks down to a green (acceptable) level, however there will be occasions when processing must take place for

legal/best interest reasons and so some processing with risks will go ahead and have to be accepted into the project. All solutions and mitigating actions must first be considered, tried and applied if possible.

• **RED** - Where an assessment outcome is Red, it indicates that either or both impact and/or likelihood scores are unacceptable and that complete solutions and mitigating actions would be required to bring both indicators down to an acceptable level. Some processing activities are eliminated at this point as the impact to individuals is considered to high risk to proceed.

However, in instances where the activity is essential or is a legal requirement, the proposed solutions and mitigating actions are applied and a further PIA to see if the subsequent PIA results in a Green and/or acceptable level of risk. If a high risk still exists and the processing activity is authorised, we always consult the Supervisory Authority (SA) prior to processing and advise that the PIA indicates that the processing would result in a high risk and there is an absence of measures that can be taken mitigate the risk. You should then await written advice from the SA and provide all information requested by them during this period.

The above process enables us to devise ways to reduce or eliminate privacy risks and assess the costs and benefits of each approach, as well as looking at the impact on an individual's privacy and the effect on the processing activity outcomes. This enables us to document our identification and assessment of the risk, the solutions and mitigating actions used to reduce or eliminate the risk and records privacy risks which have been accepted as necessary for the project to continue.

A public list of the kind of processing operations which are subject to a PIA will be published. Once published we will add the areas on the list to this document.

DATA SUBJECT RIGHTS PROCEDURES

11. CONSENT & THE RIGHT TO BE INFORMED

The collection of personal and sometimes special category data is a fundamental part of the products/services offered by our organisation and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the UK GDPR.

Where processing is based on consent, the consent request is: -

- Clear, transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms

• In an easily accessible format with the purpose for data processing attached to that consent
• Clear and distinguishable from any other matter included and/or documented alongside the consent

Our organisation maintains rigid records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent as it is to give consent.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorised prior to being circulated.

Where processing is based on consent and the personal data relates to a child who is below the age of 16 years, such processing is only carried out by our organisation where consent has been obtained by the holder of parental responsibility over the child.

Consent to obtain, process, store and share (where applicable), is obtained by our organisation through: -

1. Face-to-Face
2. Telephone
3. In Writing
4. Email

Points 1-4 are enforced using scripts, checklists, on-screen prompts and signed customer agreements, to ensure that consent has been obtained and to remind employees of their additional consent obligations, as below.

Privacy Notices are used in all forms of consent to ensure that we are compliant in disclosing the information required in the UK GDPR in an easy to read and accessible format.

11.1 INFORMATION PROVISIONS

Where consent is obtained; employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc) provide the below information in all instances, in the form of a consent/privacy notice: -

• The identity and the contact details of the controller and, where applicable, of the controller's representative
• The contact details of our data protection officer
• The purpose(s) of the processing for which the personal information is intended
• The legal basis for the processing
• Where the "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party", details of the legitimate interests
• The recipients or categories of recipients of the personal data (if applicable)
• The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
• The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
• Where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
• The right to lodge a complaint with the Supervisory Authority
• Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
• The existence of any automated decision-making, including profiling, and explanatory information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from the date of consent, unless there is a legal requirement to keep the information longer.

11.1.1 PRIVACY NOTICES

Where our organization obtains personal data from a data subject or a third-party about the data subject, we utilise Privacy Notices to provide the information set out in section 9.1 of this policy and pursuant to the UK GDPR. Our privacy notice is easily accessible, legible, jargon-free and inclusive of all information and is available in several formats as applicable to the method of data collection: -

• Via our website
• In our Privacy Notice

• Worded in full in agreements, contracts, forms and other materials where data is collected in writing or face-to-face
• Verbally via telephone or face-to-face
• Sometimes Printed media, adverts and financial promotions

With lengthy content being provided in the privacy notice and with informed consent being based on its contents, we have tested, assessed and reviewed our privacy notice to ensure usability, effectiveness and understanding.

Our Privacy Notice:

Our organisation is committed to protecting the privacy of your personal information. Our company is registered with the Information Commissioners Office (ICO) and complies with the Data Protection Act 2018 and with the data protection principles set out in the Act and the UK General Data Protection Regulations (GDPR).

Collection of Information – your consent

We may collect personal information from you if you provide it voluntarily.

If you do provide personal information to use, we will assume that you have read this Policy and have consented to us using your personal information in the ways described in this Policy and at the point where you give us your personal information.

If, after providing us with personal information, you later decide that you do not want us to use it for particular purposes, then please write to us at the appropriate address.

Reasons for Collection of your Information

In the course of our dealing with you we may collect and process certain information about you, including your name, date of birth, address, contact details (including your email address and contact telephone number), payment details (where applicable), any benefits you receive or are entitled to (including disability benefits) (where applicable), and other information about you and your property in respect of which services and products may be provided. Your personal information may be used by us, our employees, contractors or agents to:

• identify you during any communication between you and us;
• assess eligibility for services and products (whether provided by us or on our behalf);
• communicate with you to arrange the provision of such services and products;

- administer and provide such services and products;
- detect and prevent loss, fraud and other criminal activity;
- carry out credit reference checks;
- carry out market research and to help us review, develop and improve the services and products we offer; and
- contact you (in accordance with your preferences), by post, telephone, SMS, email and other electronic means with information about products, services, promotions, and offers that may be of interest to you.

In the event that we sell or buy any business or assets, we may disclose personal information held by us to the prospective seller or buyer of such business or assets. If we or substantially all of our assets are acquired by a third party, personal information held by us will be one of the transferred assets.

Your personal information may also be used by us, our employees or agents if we are under a duty to disclose or share your personal information in order to comply with any legal obligation, or in order to enforce any agreement we have with or otherwise concerning you, or to protect our rights, property or safety or those of our customers, employees or other third parties.

With whom do we share your personal information?

Third parties such as funders, grants, BEIS, TrustMark, Scheme Providers.
In connection with the above purposes, your personal information may be transferred to, or otherwise processed by third party service providers acting on our behalf, our agents and law enforcement authorities (including the police).

Access to Information

The UK GDPR gives you the right to access information held about you. You have the right to ask for a copy of the personal information held about you. You also have the right to ask for inaccuracies in information to be corrected. Access request fees are normally provided free of charge, but we reserve the right to apply an administration fee in certain cases if we consider the request to be unreasonable. A copy of the information held about you by us can be requested by writing to us at the address shown.

Transfer of Information Abroad

We will not transfer your personal information outside the UK or to any current or former member of the EU, or outside of the EEA or the EFTA without first obtaining your consent.

Change of Policy

We may occasionally change the Privacy Policy to reflect customer and company feedback. Any changes will be shown on this page.

Dealing with Data Protection Complaints

We aim to comply fully with our obligations under the Data Protection Act (DPA) 2018 and the UK GDPR. If a customer has any questions or concerns regarding our company's management of personal data including their right to access data about themselves, then they should contact the director who is responsible for ensuring our company is compliant with data protection.

If our company holds inaccurate information, then the customer should write to our company at the address shown providing the director with any evidence to show what the information should say keeping copies of the correspondence. If after a reasonable amount of time (28 days is recommended) the information has not been corrected, then the customer can make a complaint.

There are two courses of action:

1. Contact the director to process the complaint.
2. If the customer is still dissatisfied, they can go directly to the Information Commissioner, the independent body that oversees data protection and the UK GDPR. They can be contacted on 0303 123 1113 or their website is www.ico.org.uk .

Ongoing Compliance

1. Privacy Notices are drafted by a competent member of staff using the UK GDPR requirements and with Supervisory Authority guidance

2. We may utilise a select customer base to test the Privacy Notice in its varying formats and provide a feedback form for completion, verifying the below points: -

a. How did you use the Privacy Notice (e.g. website, agreement, orally)?
b. Did you find the information in the Privacy Notice easy to read, understand and access?
c. Did you gain a full understanding of how we intend to use your data, who it will be shared with and what your rights are?
d. Did you feel confident in giving consent to use your personal data after reading the notice information?
e. Was there anything you did not understand?

f. Did you find any errors?
g. What, if anything, would you like to see changed about the Privacy Notice?

3. All feedback responses are saved with a copy of the used Privacy Notice and improvements are made and recorded where applicable

4. Re-testing is carried out on a new set of customers to ensure variety and independent assessment and verification

5. After a successful test, the acceptable Privacy Notice is rechecked against the UK GDPR and Supervisory Authority regulations and guidelines to ensure it still complies and is adequate and effective

6. The final Privacy Notice(s) are then authorised by Senior Management/Director(s) before being rolled out

Where we rely on consent to obtain and process personal information, we ensure that it is: -

- Displayed clearly and prominently
- Asks individuals to positively opt-in
- Gives them sufficient information to make an informed choice
- Explains the different ways we will use their information
- Provides a clear and simple way for them to indicate they agree to different types of processing
- Includes a separate unticked opt-in box for direct marketing

11.2 PERSONAL DATA NOT OBTAINED FROM THE DATA SUBJECT

Where our organization acts in its capacity as a data controller and where it has not obtained personal data directly from the data subject, our organization ensures that the information noted in section 9.1.1 of this policy is provided to the data subject within 30 days of our obtaining the personal data.

In addition to the information that is provided to the data subject as set out in section 9.1.1, where the information has been obtained from a third-party, also advises the individual about: -

- The categories of personal data
- The source the personal data originated from and whether it came from publicly accessible sources

Where the personal data is to be used for communication with the data subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication or disclosure. Where our organization intends to further process any personal data for a purpose other than that for which it was originally obtained, we communicate this intention to the data subject prior doing so and where applicable, process only with their consent.

Whilst we follow best practice in the provision of the information noted in section 9.1.1 of this policy, we reserve the right not to provide the data subject with the information if: -

- They already have it and we can evidence their prior receipt of the information
- The provision of such information proves impossible and/or would involve a disproportionate effort
- Obtaining or disclosure is expressly laid down by Union or Member State law to which it is subject and which provides appropriate measures to protect the data subject's legitimate interest
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy

12. THE RIGHT OF ACCESS

We have ensured that appropriate measures have been taken to provide information and any communication relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means if authorised by the data subject and with prior verification as to the subject's identity (i.e. verbally, electronic).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request was received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in wiring throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority. Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: -

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- If the data has or will be disclosed to a third countries or international organisations and the appropriate safeguards pursuant to the transfer
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority
- Where personal data has not been collected by our organisation from the data subject, any available information as to the source and provider
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

12.1 DATA PORTABILITY

Our organization provides all personal information pertaining to the data subject, to them on request and in a format that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services. Where requested by a data subject for whom we hold consent to process and share their personal information and when processing is carried out by automated means, we will transmit the personal data directly from ourselves to a designated controller, where technically feasible.

To ensure that we can comply with the UK GDPR concerning data portability, we keep a machine-readable version of all personal information and utilise the below formats for compliance: -

- HTML
- XML

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

13. RECTIFICATION & ERASURE

13.1 CORRECTING INACCURATE OR INCOMPLETE DATA

All data held and processed by our organization is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller inform us that the data, we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

Where we are notified on incomplete data, we will complete the information as directed by the data subject, including adding an addendum or supplementary statement where applicable. If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

13.2 THE RIGHT TO ERASURE

Also, known as *'The Right to be Forgotten'*, our organization ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed. All personal data obtained and processed by our organization is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

These measures enable us to comply with a data subject's right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

Where we receive a request to erase and/or remove personal information from a data subject, the below process is followed: -

1. The request is allocated to the member of staff responsible and recorded on the Erasure Request Register
2. The member of staff locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure: -
    a. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
    b. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
    c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing
    d. the personal data has been unlawfully processed
    e. the personal data must be erased for compliance with a legal obligation
    f. the personal data has been collected in relation to the offer of information society services to a child
4. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
5. The member of staff writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure
6. Where our organization has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. Such refusals to erase data include: -

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health

• For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
• For the establishment, exercise or defence of legal claims

14. THE RIGHT TO RESTRICT PROCESSING

There are certain circumstances where our organization restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subjects request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit. Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted, it is only stored and not processed in any way.

Our organisation will apply restriction to data processing in the following circumstances: -

• Where an individual contests the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
• Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether we have legitimate grounds to override those of the individual
• When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure
• Where we no longer need the personal data but the data subject requires the data to establish, exercise or defend a legal claim

The member of staff responsible reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third-parties. Where data is restricted and we have disclosed such data to a third-party, we will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. We also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

15. OBJECTIONS AND AUTOMATED DECISION MAKING

Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material and provide an online objection form where processing is carried out online. Individuals have the right to object to: -

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- Direct marketing (including profiling)
- Processing for purposes of scientific/historical research and statistics

Where our organization processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subjects' objection will only be considered where it is on 'grounds relating to their particular situation'. We reserve the right to continue processing such personal data where: -

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise or defence of legal claims

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, our organization will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

We have carried out a system audit to identify automated decision-making processes that do not involve human intervention. We also assess new systems and technologies for this same component prior to implementation. Our organization understands that decisions absent of human interactions can be biased towards individuals and we aim to put measures into place to safeguard individuals where appropriate. Via our Privacy Notices, in our first communications with an individual and on our website, we advise individuals of their rights not to be subject to a decision when: -

- It is based on automated processing
- It produces a legal effect or a similarly significant effect on the individual

In limited circumstances, our organization will use automated decision-making processes within the guidelines of the regulations. Such instances include: -

- Where it is necessary for entering into or performance of a contract between us and the individual
- Where it is authorised by law (e.g. fraud or tax evasion prevention)
- When based on explicit consent to do so
- Where the decision does not have a legal or similarly significant effect on someone

Where our organisation uses, automated decision-making processes, we always inform the individual and advise them of their rights. We also ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

OVERSIGHT PROCEDURES

16. SECURITY & BREACH MANAGEMENT

Alongside our 'Privacy by Design' approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred.

We carry out information audits to ensure that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s).

We have implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including: -

- Encryption of personal data in some instances
- Restricted access
- Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Disaster Recovery and Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Audit procedures and stress testing on a regularly basis to test, assess, review and evaluating the effectiveness of all measures and compliance with the data protection regulations and codes of conduct

• Frequent and rolling training programs for all staff in the UK GDPR, its principles and applying those regulations to each role, duty and the company as a whole
• Staff assessments and testing to ensure a high level of competency, knowledge and understanding of the data protection regulations and the measures we have in place to protect personal information
• Recheck processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal, it is rechecked and authorised

We have dedicated procedures for identifying, assessing and investigating compliance breaches and use a Breach Register to record all information for consistency and compliance. Where a breach involves personal data, the member of staff who undertakes responsibility will assist the Compliance Officer in the investigating and propose solutions and mitigating actions to prevent further breaches. The full scope of the process can be found in our Breach Procedure Flowchart.

In the case of a personal data breach, we ensure that the Supervisory Authority is notified of the breach with immediate effect and at the latest, within 72 hours after having become aware of the breach. The Supervisory Authority is kept notified throughout the investigation and is provided with a full report, including outcomes and mitigating actions as soon as it is available. Where a breach is assessed and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority.

However, breach incident procedures and an investigation is still carried out in full and the outcomes and report are made available to the Supervisory Authority if requested. If for any reason, it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for the delay.

Where the breach has occurred with a processor appointed by our organisation, our agreement outlines that they shall notify us without undue delay after becoming aware of a personal data breach.

The notification to the Supervisory Authority will contain: -

• A description of the nature of the personal data breach
• The categories and approximate number of data subjects affected
• The categories and approximate number of personal data records concerned
• The name and contact details of our relevant point of contact (for obtaining further information)
• A description of the likely consequences of the personal data breach

• A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written format and in a clear and legible format. The notification shall include the nature of the personal data breach, the name and contact details of our person responsible, a description of the likely consequences of the breach and a description of the measures taken or proposed, to address the breach.

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational protection measures which render the data unintelligible to any person who is not authorised to access it (i.e. encryption, data masking etc) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

17. TRANSFERS & DATA SHARING

Our organisation takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred. Data transfers within the UK and EU are deemed less of a risk than a third country or an international organisation, due to the UK GDPR covering the former and the strict regulations applicable to all EU Member States.

All our data is obtained and transferred ONLY within the UK.

In the unlikely event where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we will utilise a process that ensures such data is encrypted with a secret key. We will use approved, secure methods of transfer and have dedicated points of contact with each Member State organisation with whom we deal. All data being transferred is noted on our information audit so that tracking is easily available and authorisation is accessible.

We will only conduct transfers of personal data to third countries or international organisations where the Commission has advised that adequate levels of protections are in place.

17.1 APPROPRIATE SAFEGUARDS

In the absence of a decision by the Commission on an adequate level of protection by a third country or an international organisation, we would restrict transfers to those that are legally binding or essential for the provision of our business obligations or in the best interests of the data subject. In such instances, we would develop and implement appropriate measures and safeguards to protect the data, during transfer and for the duration it is processed and/or stored with the third country or international organisation.

Such measures include ensuring that the rights of data subjects can be carried out and enforced and that effective legal remedies for data subjects are available. The appropriate safeguards can be provided without Supervisory Authority authorisation by: -

- A legally binding and enforceable instrument between public authorities or bodies
- Binding corporate rules
- Standard data protection clauses adopted by the Commission
- Standard data protection clauses adopted by a Supervisory Authority and approved by the Commission
- An approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights
- An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights

With authorisation from the Supervisory Authority, the appropriate safeguards may also be provided for by: -

- Contractual clauses between our organisation and the controller, processor or the recipient of the personal data in the third country or international organisation
- Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights

Our organisation does not transfer personal data to any third country or international organisation without one or more of the above safeguards being in place or without the authorisation of the Supervisory Authority where applicable. We verify that any safeguards,

adhere to the UK GDPR Principles, enforce the rights of the data subject and protect personal information in accordance with the Regulation.

We ensure that any agreement, contract or binding corporate rules for transferring personal data to a third country or international organisation, are drafted in accordance with any Supervisory Authority and/or the Commission's specification for format and procedures (where applicable).

As a minimum standard, we verify that the below are specified: -

- The structure and contact details of the group engaged in the activity and of each of its members
- The data transfers or set of transfers, including: -
    - the categories of personal data
    - the type of processing and its purposes
    - the type of data subjects affected
- the identification of the third country or countries in question
- Their legally binding nature, both internally and externally
- The application of the general data protection principles, in particular: -
    - purpose limitation
    - data minimisation
    - limited storage periods
    - data quality
    - data protection by design and by default
    - legal basis for processing
    - processing of special categories of personal data
    - measures to ensure data security
    - the requirements in respect of onward transfers to bodies not bound by the binding corporate rules
- The rights of data subjects regarding processing and the means to exercise those rights, including the right: -
    - not to be subject to decisions based solely on automated processing (incl. profiling)
    - to lodge a complaint with the competent Supervisory Authority and before the competent courts of the Member States
    - to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules
- Our acceptance (and that of any processor acting on our behalf) of liability for any breaches of the binding corporate rules by the third country or international organisation to whom the data is being transferred (with exemption from that

liability, in whole or in part, only where we prove that we are not responsible for the event giving rise to the damage)

• How the information on the binding corporate rules and the information disclosures is provided to the data subjects (with particular reference to the application of the UK GDPR Principles, the data subjects rights and breach liability)

• The tasks of any Data Protection Officer and/or person(s) in charge of monitoring compliance with the binding corporate rules, as well as monitoring training and complaint-handling

• The complaint procedures

• The mechanisms within the group engaged in the activity, for ensuring the verification of compliance with the binding corporate rules, including: -

- data protection audits
- methods for ensuring corrective actions to protect the rights of the data subject
- providing the Data Protection Officer and controlling board with such verification results

• The mechanisms for reporting and recording changes to the rules and reporting those changes to the Supervisory Authority

• The cooperation mechanism with the Supervisory Authority to ensure compliance by any member of the group, in particular by making available to the Supervisory Authority, the results of verifications of the measures referred to above

• The mechanisms for reporting to the competent Supervisory Authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules

• The appropriate data protection training to personnel having permanent or regular access to personal data

17.2 TRANSFER EXCEPTIONS

Our organisation DOES NOT transfer data outside of the UK. We understand that we are not to transfer any personal information to a third country or international organisation without an adequacy decision by the Commission or with Supervisory Authority authorisation and the appropriate safeguarding measures; unless one of the below conditions applies. The transfer is: -

• made with the explicit consent of the data subject, after having been informed of the possible risks and the absence of an adequacy decision and appropriate safeguards

• necessary for the performance of a contract between the data subject and our organisation or the implementation of pre-contractual measures taken at the data subject's request
• necessary for the conclusion or performance of a contract concluded in the interest of the data subject between our organisation and another natural or legal person
• necessary for important reasons of public interest
• necessary for the establishment, exercise or defence of legal claims
• necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
• made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register). Transfer made under this exception must not involve the entire personal data or categories of the personal data in the register and if the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

Where a transfer is not valid and none of the above derogations apply, our organisation complies with the provision that a transfer can still be affected to a third country or an international organisation where all the below conditions apply. The transfer: -

• cannot be made by a public authority in the exercise of its public powers
• is not repetitive
• concerns only a limited number of data subjects
• is necessary for the purposes of compelling legitimate interests pursued by our organisation which are not overridden by the interests or rights and freedoms of the data subject
• Our organisation has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment, provided suitable safeguards with regard to the protection of personal data

Where the above transfer must take place for legal and/or compelling legitimate reasons, the Supervisory Authority is notified of the transfer and the safeguards in place, prior to it taking place. The data subject in such instances is provided with all information disclosures as well as being informed of the transfer, the compelling legitimate interests pursued and the safeguards utilised to affect the transfer.

18. AUDITS & MONITORING

This policy and procedure document details the extensive controls, measures and methods used by our organisation to protect personal data, uphold the rights of data subjects,

mitigate risks, minimise breaches and comply with the UK GDPR and associated laws and codes of conduct. In addition to these, we also carry out regular audits and compliance monitoring processes with a view to ensuring that the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The member of staff who takes responsibility has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management Team where applicable. Data minimisation methods are frequently reviewed and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded and copies provided to Senior Management and are made readily available to the Supervisory Authority where requested.

The aim of internal data protection audits is to: -

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance
- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and action plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data
- To monitor compliance with the UK GDPR and demonstrate best practice

19. TRAINING

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the UK GDPR requirements and its principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role. Our Training & Development Policy & Procedures and Induction Policy detail how new and existing employees are trained, assessed and supported and include: -

- GDPR Workshops & Training Sessions
- Specific GDPR E-Learning Training Courses
- Assessment Tests
- 1:1 Support Sessions
- Scripts and Reminder Aids
- Access to UK GDPR policies, procedures, checklists and supporting documents

20. PRIVACY AND ELECTRONIC COMMUNICATIONS (PECR)

Our organisation confirms that it complies with all regulations and laws made under the Privacy and Electronic Communications Regulations 2003, in respect to any related business activity.

We confirm that where individuals are concerned, we will only send direct marketing media (emails, calls or postal), when solicited (given direct prior consent) and will retain proof of all such consent for recording and auditing purposes.

Where any marketing material is delivered using an automated calling system, it will be done so only with the individual prior consent and any request to remove such consent will be recorded and applied with immediate effect.

No unsolicited tele-sales or marketing calls will be made where an individual is registered on the TPS (Telephone preference service) and any staff identified to be doing so will be subject to disciplinary action.

Any solicited tele-sales or marketing calls made by our organisation will be in accordance with the below requirements: -

- Agents will identify themselves and the firm form which they are calling from
- Agents will disclose the nature and purpose of the call
- If asked, the agent will provide a valid business address and contact telephone number

No unsolicited sales or marketing attempts will be made by fax without the recipients' prior consent.

Any sales or marketing emails will: -

- Identify the name of the firm, their trading address and a valid contact number
- Contain an opt-out request for the individual to unsubscribe to any further emails
- Ensure our business has obtained the necessary consent from individuals for marketing in compliance with data protection legislation and PECR (Privacy and Electronic Communications Regulations).

21. PENALTIES

Our organisation understands our obligations and responsibilities under the UK GDPR and Supervisory Authority and comprehend the severity of any breaches under the Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and

enforce fines and penalties on us where we breach the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach.

22. RESPONSIBILITIES

Our organisation has appointed a senior member of staff responsible for Data Protection whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection. This person will work in conjunction with the Compliance Officer to ensure that all processes, systems and staff are operating compliantly and within the requirements of the UK GDPR and its principles.

This person has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the UK GDPR and our own internal objectives and obligations.

Staff who manage and process personal or special category information (which is unlikely in our business) will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledgeable for the role they undertake.

The aims of this policy will be communicated to new staff upon joining and at annual staff reviews.

The policy will be reviewed at least on an annual basis.

Eco Efficient Home Solutions Ltd t/as EEH Solutions Integrated Management System		
Document Title:	**General Data Protection Regulation Policy and Procedure**	
Ref. No.:	**GDPP012**	
Document Users / Security Class:	**All Users**	
Next Review Date	**One Year**	

Last reviewed: 1st January 2024

Next review: 1st January 2025

Name: Raja Naveed
Signature: Raja Naveed
Position: Director

Document Author:	David Mooney		
Document Approver:	Raja Naveed	**Controller:**	Data Protection

----------END OF DOCUMENT----------

Eco Efficient Home Solutions Ltd t/as EEH Solutions Integrated Management System		
Document Title:	**General Data Protection Regulation Policy and Procedure**	
Ref. No.:	**GDPP012**	
Document Users / Security Class:	**All Users**	
Next Review Date	**One Year**	

Version Number	Amendment	Date
1.0	New document. Document introduced in order to eventually replace GDPP020 – Data Protection Procedure due to new GDPR regulations that come into force in May 2018.	7th June 2017
1.1	Reviewed document and added "2. Purpose" added access to e-learning courses; "6. & 6.2" Added reference to Data Protection Act 2018; "19 – Training" added specific GDPR e-learning courses.	28th February 2019
1.2	Document reviewed. General update anticipating impact of Brexit arrangements to Section 5; Appointment of DPO to Section 8.	28th February 2020
1.3	Document reviewed. (1) Foreword section completely revised in line with UK leaving the EU and the EU GDPR no longer applying to the UK and description of UK GDPR; (2) Reference now made to UK GDPR throughout; (3) Extended 3. SCOPE description so we can still transfer data to and from Europe; (4) Extended 5. DATA PROTECTION REGULATION BACKGROUND description to reflect the Brexit changes.	28th February 2021
1.4	Document reviewed. (1) Added that on 28th June 2021, the EU approved adequacy decision for the EU GDPR and the Law Enforcement Directive (LED). This means data can continue to flow as it did before, in the majority or circumstances. Both decisions are expected to last until 27th June 2025. Most EEA processors will be able to send personal data back to UK controllers with no restrictions. (The EU GDPR is an EU Regulation and it no longer applies to the UK. We operate inside the UK, and need to comply with the Data Protection Act 2018 (DPA 2018). 2) Removed The EU GDPR will still apply to any organisations in Europe who send us data, so we may need to help them decide how to transfer personal data to the UK in line with the UK GDPR, if the trade deal bridge ends without adequacy.	28th February 2022
1.4	Document reviewed and no changes made.	28th February 2023

1.5	Document reviewed and (1) amended review period to the 1st January to align with other policies and procedure reviews. (2) Expanded on Policy Statement to highlight the UK GDPR 7 principles.	1st January 2024