Privacy policy

WWW.EGOTECHNOLOGY.CO.UK

Online and privacy policy

European GDPR Regulations and UK Data Protection Act 2018 Business Compliance Document

3. Overview

3.1 This document has been prepared bespoke to the business activity of Ego Recycling Ltd hereinafter referred to as We and Us.
3.2 This document has been prepared and approved by Ego Recycling Ltd following a data
audit conducted on 25th November 2019 in accordance with the GDPR.
3.3 The purpose of this document is to demonstrate the Data Protection protocols employed by Ego Recycling Ltd and will be kept updated as appropriate.
3.4 Ego Recycling Ltd is a Data Controller under the provisions of the GDPR and the Data Protection Act 2018 and is registered with the UK Information Commissioners office.
ICO Registration Number: ZA 504114
3.4 The Data Processing Contact for this business is: M Austin
3.5 In the course of business, We may act as Data Processor under contract for clients and other third parties in business. However, this document relates to activities conducted as Data Controller in our own capacity.
4. Privacy Policy Statement
4.1 As a Data Controller, We will take all the necessary steps to comply with the Data Protection Act 2018 and other relevant legislation and regulations when handling any personal data which is provided to us.
This includes ensuring that data under our control is:
4.1.1 Fairly and lawfully processed.
4.1.2 Processed for limited purposes.
Document Version 1.1
4.1.3 Adequate, relevant and not excessive.
4.1.4 Accurate and not kept for longer than necessary.
4.1.5 Processed in accordance with the prescribed rights.
4.1.6 Secure and not transferred to countries outside the European Economic Area without appropriate safeguards.
4.2 Our data processing contact can be contacted at the above address for the following reasons: -
4.2.1 To obtain a copy of the personal data we hold about an individual. 4.2.2 If someone believes any personal data or information which we hold about them is incorrect or incomplete. NB: Any information or data which is found to be incorrect will be corrected as soon as possible.
4.2.3 To have an individual's personal data removed entirely from our systems.

4.3 There is no charge for these services. As soon as we are satisfied as to the identity of the person making the request, we will send them, within a month of the request a copy of all the data we hold relating to them.
4.4 As soon as we are satisfied as to the identity of the person making a removal request and the data is not required to be kept for any other lawful reason or purpose it will be removed from our systems forthwith.
4.5 As soon as we are satisfied as to the identity of the person making a rectification request the data in question will be corrected or rectified as appropriate in our systems forthwith.
4.6 If anyone is unhappy with any of the responses given by us, they may complain to the Regulator at the Information Commissioners Office on 0303 123 1113.
Document Version 1.1
5. Data under Control – Lawful bases in parentheses.
5.1 Following the completion of an information audit and consideration of the rules regarding completion of a Data Protection Impact Assessment, we have concluded that the Data under our control are identified as arriving from Nine separate sources.
5.1.1 Prospective and existing Customers providing their information for the purposes of contracting with us for goods or services. (Contract)
5.1.2 Prospective and existing Customers providing their personal information either Online or Offline including Social Media, telephone and by written means to ourselves or third parties to request information regarding our available products and services. (Consent)
5.1.3 Customers information received both Online or Offline including Social Media, telephone and by written means to Ourselves or third parties to facilitate contractual obligations regarding our products and services. (Contract)
5.1.4 People providing their personal information either Online or Offline including Social Media, telephone and by written means because they are interested in working with us or learning more about working with us. (Consent)
5.1.5 Online or Offline face to face meetings with people who provide their personal information to us for the purposes of later contact regarding products and services provided by us. (Consent)
5.1.6 Our Employees who provide their details for our information for the purposes of working with us. (Legal Obligation)
5.1.7 Suppliers of products and services to us who provide information of themselves or relevant individuals who assist them to provide us with products and services on their behalf. (Contract)
5.1.8 People identified through the use of our CCTV systems. (Legitimate Interest)
Document Version 1.1
6. Lawful Bases for processing
6.1 We understand there are 6 Lawful bases for data processing:
6.1.1 Consent: [Art 6 (1) a GDPR]
Where we process information with the specific consent of the individual concerned, whether for our services or for referral to our professional partners.
6.1.2 Contract: [Art 6 (1) b GDPR]
The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the direct request of the data subject prior to entering into a contract.

6.1.3 Legal Obligation: [Art 6 (1) c GDPR]
The processing is necessary for a compliance with a legal obligation to which the controller is subject.
6.1.4 Vital Interests: [Art 6 (1) d GDPR]
The processing is necessary in order to protect the vital interests of the data subject or of another natural person.
6.1.5 Public Task: [Art 6 (1) e GDPR]
The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6.1.6 Legitimate Interests: [Art 6 (1) f GDPR]
The processing is necessary for the purposes of the legitimate interests pursued by the controller 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.
NB: This Basis is only available following a Legitimate Interests Assessment and the application of the three part Legitimate Interests Assessment Test.
6.2 We also understand the principles relating to Special Category Data, being the type of data which could create more significant risks to a person's fundamental rights and freedoms.
6.3 We are involved with Special Category data both for our employees and with clients. Consequently, when we are dealing with sensitive data our subsidiary legal basis for employees are described in Section 11 of this document and for clients the lawful bases are those provided for in Article 9(2) of the GDPR
7. Children's Data
7.1 As a general rule we do not contract with children to provide products or services.
7.2 We may record details of client's children if relevant and appropriate to our business activity or for the purpose of giving the client advice and may subsequently reference such children in our records. In all cases where a child is under 13 years, we receive parental consent to record the child's details.
8. Individuals Rights
8.1 We are aware of the individual's rights protected by the GDPR and Data Protection
Act 2018 as being the following:

- 8.1.1 The right to be informed
- 8.1.2 The right of access
- 8.1.3 The right to rectification
- 8.1.4 The right to erasure
- 8.1.5 The right to restrict processing
- 8.1.6 The right to data portability
- 8.1.7 The right to object
- 8.1.8 The right not to be subject to automated decision making, including profiling.

8.2 These rights are protected and included in our Privacy policy statement.
8.3 We do not conduct automated data processing activity or operate within areas where Data Portability would be encountered
8.4 In our Online presence and Website there is provided a method for contacting us and requesting Access to any data held by ourselves subject to the usual legal controls.

9. Subject Access Requests

We have determined a policy to comply with Subject Access Requests. It is referenced in our Privacy Policy and will consist of the following:

9.1 Request for information held on a Data Subject

9.1.1 The SAR will be notified to or come to the notice of our Data Processing Contact who will:-

9.1.2 Make enquiries as to the identity of the enquirer and contemporaneously establish the type and quantity of relevant Data under Control by Us.

9.1.3 Gather or arrange to be gathered the information in preparation for dispatch to the enquirer.

9.1.4 Supervise the dispatch of the data within the prescribed timescale of one month and record the details of the SAR and the fact of its completion.

9.2 Request for the Rectification or Removal of Data

9.2.1 The SAR will be notified to or come to the notice of our Data Processing Contact who will:

9.2.2 Make enquiries as to the identity of the enquirer and contemporaneously establish the type and quantity of relevant Data under Control by Us.

Then EITHER:

a) The Data will be checked for accuracy and rectified where necessary. Or,

b) The Data will be checked for lawful reasons to retain, then if there are none, gathered together and removed from Our systems and records if applicable.

9.2.3 Notify the enquirer as to the changes (if any) made within the prescribed timescale of one month.

9.2.4 Record the details of the SAR and the fact of its completion.

9.3 Identification

9.3.1 To access what personal data is held, identification will be required. We will accept the following forms of ID when information on personal data is requested:

a) A National ID card.
b) A Driving Licence.
c) A Valid Passport.
d) A Birth Certificate
e) A Utility bill not more than three months old.

9.3.2 A minimum of one piece of photographic ID listed above and one other document from the list is required.

9.3.3 Until We are satisfied with the documents provided, further identification may be sought before personal data can be released.

9.3.4 Failure or refusal to provide the requested identification or if the identification provided is not satisfactory, no personal data held by Us will be released.

9.3.5 In the circumstances outlined in clause 9.3.4 above our refusal to comply with the request will be recorded and the enquirer informed.

9.3.6 Enquiries by third parties will also require identification checks and confirmation by the primary Data Subject.

9.3.7 Requests which are manifestly unfounded or excessive will incur a charge which will be calculated taking into consideration the administrative task involved in complying with the request.

10. Data Security: Transfer, Storage and Retention Policies

We recognise the need for structural and organisational Data Security. The following policies deal with the forward planning and organisational security arrangements.

10.1 Data Transfers.

10.1.1 Personal Data under our control will only be transferred to a third party organisation under the terms of a written Data Processors Contract.

10.1.2 Personal Data in emails will be encrypted where possible where it is not possible the email should be encrypted. Attachments to emails containing Personal Data will always be encrypted.

10.1.3 Personal data must not be transferred over a wireless network if a hardwired network is available.

10.1.4 Where it is necessary to transfer the password or encryption code for an email it must not be transferred with the encrypted email.

10.1.5 Passwords if transferred by email must be sent over a different email system to that of the encrypted email. Where this is not possible another means must be considered E.g. Voice or SMS transfer.

10.1.6 SMS transfers of Personal Data should be kept to a minimum and only sent to telephone numbers which have previously been satisfactorily identified as the correct recipient and ideally after a voice call on that particular line.

10.1.6 Transfer of hard copy documents must be achieved through personal physical contact or if using the Royal Mail system by Special Delivery only.

10.1.7 Personal Data contained on removable media must be encrypted and its transfer achieved through personal physical contact or if using the Royal Mail system by Special Delivery only.

10.2 Data Storage

10.2.1 Personal Data is held by us in secure electronic devices such as computers, Ipads, mobile phones and separate back up devices and servers.

10.2.2 Data is also held by us in paper form in files relating to individuals, which are secured by virtue of the physical security at their location.

10.2.3 We have no plans to introduce new technology such as face recognition, biometrics or fingerprint recognition into our Data processing activities but if such a change is made or planned to be made We will complete a detailed Data Protection Impact Assessment and update this policy statement.

10.2.4 Hardcopies of Personal Data must be kept securely in a locked cupboard or secure filing system.

10.2.5 Removable Media containing Personal Data must be kept securely in a locked cupboard or secure filing system.

10.3 Data Retention

10.3.1 We will retain the data of data subjects for no longer than is necessary for the purposes for which the personal data are processed. We have established the following criteria to assist in determining the relevant time scale.

10.3.2 Speculative enquiries for information, the data will be retained for 12 months, in case of a follow up enquiry. E.g. Website enquiries.

10.3.3 Contractual data retained until 7 years after the end of contractual obligations. E.g. Customers, suppliers etc.

10.3.4 For repeat clients or those with additional or repeating expectations, their data will be kept until the expectations no longer exist plus 6 years in accordance with the details of Paragraph 10.3.3 above.

10.3.5 If we have a Legal obligation to retain any data it will be held securely until the obligation no longer exists plus 7 years in accordance with the details of Paragraph 10.3.3 above.

11. HR & Payroll Policies

As a core activity within our business We process data for the purposes of our Human Resources function and Payroll function.

11.1 The lawful authority we rely on for processing this personal data is article 6(1)(b) of the GDPR, which relates to processing necessary to perform a contract or to take steps as requested, before entering a contract.

11.2 The lawful authority we rely on to process any information provided as part of an employment application which is special category data, such as health, religious or ethnic information is Article 9(2)(b) of the GDPR, which also relates to our obligations in employment and the safeguarding of the employee's fundamental rights and article 9(2)(h) for assessing an individual's work capacity as an employee.

11.3 Also, Schedule 1 part 1(1) and (2)(a) and (b) of the Data Protection Act 2018 which relates to processing for employment, the assessment of working capacity and preventative or occupational medicine.

11.4 We recognise that staff are entitled to the same data access rights listed above and should follow the procedure laid out in the Subject Access Requests section of this policy document.

11.5 Recruitment

11.5.1 We use the information provided during the recruitment process to progress employment applications with a view to offering an employment contract.

11.5.2 We use contact details provided to contact applicants to progress their application and the other information provided to assess suitability for the role.

11.5.3 Wedonotcollectmoreinformationthanweneedtofulfilourstatedpurposes and will not keep it longer than necessary.

11.5.4 If an individual is invited for interview we may ask for additional information such as personal referees and health information to establish fitness to work.

11.5.5 If we make a conditional offer of employment, we will ask for information so that we can carry out pre-employment checks. An individual must successfully complete pre-employment checks to progress to a final offer.

11.5.6 We must confirm the identity of our staff and their right to work in the United Kingdom and seek assurance as to their trustworthiness, integrity and reliability.

11.6 Payroll

11.6.1 To manage our Payroll function we use information provided by employees to ensure accurate and timely payment of wages and emoluments.

11.6.2 The lawful authority for this function is our contractual relationship with employees and the legal obligation we have under HMRC and other legislation.

11.6.3 We collect no more information than is necessary to perform the function.

11.6.4 We may complete the Payroll function ourselves or contract with a Data Processor to perform the function on our behalf, in which case the information transmission between ourselves and the Data Processor will be subject to strict security measures and encrypted where necessary and appropriate.

11.7 Biometric information

11.7.1 It is not our intention to operate biometric identification devices within our business operation.

11.7.2 If this policy changes, or such a change is made or planned to be made We will complete a detailed Data Protection Impact Assessment and update this policy statement accordingly.

12. Closed Circuit Television Systems (CCTV).

12.1 We operate a digital CCTV system within our premises. We understand the CCTV cameras record personal data of individuals within the premises and can therefore be the subject of a Data Access Request.

12.2 We do not use covert CCTV recording equipment. Employees and visitors to the premises are informed of the CCTV activity by virtue of this privacy policy and the use of signs in the premises.

12.3 A Legitimate Interests Assessment was conducted by Us that determined the following:

12.4 THE PURPOSE TEST

12.4.1 We wish to use CCTV cameras in our business premises to passively record the activity therein.

12.4.2 Use of CCTV will enable photographic evidence of activity within the premises should an incident occur

12.4.3 Lawful authorities such as the Police and Health & Safety investigators would benefit from the recordings in the event of an incident.

12.4.4 The CCTV system will be operated in line with the industry guidelines set out in the CCTV code of practice promulgated by the ICO.

12.4.5 The CCTV cameras are clearly visible.

12.4.6 The operation of the CCTV cameras is Signposted.

12.4.7 The CCTV cameras will not be used in a way which could create any ethical issues such as public decency.

12.5 THE NECESSITY TEST

12.5.1 Video recording in the workplace is considered a useful and necessary activity.

12.5.2 Video recording in the workplace can only be achieved using a CCTV system.

12.5.3 Using a Digital CCTV system is a proportionate and unobtrusive response to the situation.

12.6 THE BALANCING TEST

12.6.1 The CCTV cameras will only be used in operational areas of the business.

12.6.2 The cameras do not focus only on one sector of employees or visitors and are used in the manner that would, objectively be expected.

12.6.3 The CCTV data is not constantly monitored by personnel and is only used in a reactive manner should an incident occur.

12.6.4 The recordings are held digitally, password protected, accessible only by trained and approved staff members and kept for no longer than 3 months.

12.6.5 The use of the CCTV system does not impact the Data Subject or their rights and freedoms in a negative way.

12.6.6 We do not expect anyone to object to the processing of their data in this way and we recognise that CCTV data can form the basis of a Subject Access Request which can be made to us under our Policy in Section 9 of this document should a data subject have any concerns.

12.7 Consequently, it was decided that there was no infringement of the GDPR for the use of the CCTV equipment and the legal basis for their use was established as being in our Legitimate Interests for the following purposes:

12.7.1 To protect our business premises.

12.7.2 The safety of our employees and visitors to the premises.

12.7.3 To assist lawful authorities in the prevention and detection of crime.

13. Data Breaches

13.1 We have determined a policy to comply with Data Breaches as follows:

13.2 Details of the breach will be notified to or come to the notice of our Data Protection Contact who will begin an investigation into the breach to determine:-

- 13.2.1 Its existence
- 13.2.2 Its extent
- 13.2.3 Its consequences

13.3 Our Data Protection Contact will inform the ICO immediately and in any event within 72 hours if the breach is likely to result in a risk to the rights and freedoms of individuals or could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

13.4 Notify those concerned, directly if a breach is likely to result in a high risk to the rights and freedoms of individuals.

14. Data Protection Officer

14.1 We have designated a Data Protection Contact for the business, as detailed in this document at Section 3.4 above.

14.2 We are not required to formally designate a Data Protection Officer (DPO) Because we are not engaged in any of the following activities:

14.2.1 We are not a public authority.

14.2.2 We are not an organisation that carries out the regular and systematic monitoring of individuals on a large scale.

14.2.3 We are not an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

14.3 We do not believe it is necessary to appoint a DPO voluntarily but if this policy changes, or such a change is made or planned to be made, we will complete a detailed Data Protection Impact Assessment and update this policy statement accordingly.

15. International Data Processing

15.1 We do not generally operate outside of the United Kingdom but we may maintain professional contacts in other EU member States and beyond.

15.2 All Data and information collected in any State will be processed in the UK. These arrangements are generally under the legal bases of Consent or Contract with either hard copy or Online opt in signatures as appropriate.

15.3 Due to the operation of the Internet and other computer based applications Personal Data under our control may transit non EU countries.

15.4 We will only transfer data outside the EU if adequate safeguards are in place in the destination country.

15.5 The Main Establishment for Our International Data Processing is the UK.

15.6 The lead supervisory authority is UK Law and the UK Information Commissioners Office whose address is Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

16. Review and Updating
16.1 We recognise both the fluid and developing nature of Data Processing legislation and
procedures.
16.2 We have established a regular system for review and updating as required.
16.3 Our Data Processing Contact is responsible for arranging reviews of our systems and staff training in line with our established training schedule.
16.4 The Data Protection staff training schedule is established as follows:
16.4.1 Induction – On appointment or re-appointment.
16.4.2 Ongoing - On a rolling six monthly basis of knowledge checks and reminders.
16.4.2 Updating – As required consequent to changing and developing rules and procedures.
16.4.3 Our Data Protection contact has been authorised to make enquiries of our Legal advisors, if required, in the event of any queries beyond his existing understanding and knowledge.
Prepared for the business activity of: Ego Recycling Ltd Policy Active from: 9 December 2019 Update required by: 9 December 2020

1. Ego Recycling Ltd.
3 Glensyl Way Burton on Trent Staffordshire DE14 1LX
Tel: 01283 890990. Email: melissa.austin@egorecycling.com

2. Status of Key Organisational Personnel
Mr Ian Austin – Company Director
Mrs Melissa Austin – Company Director

ego

+44 (0) 1283 890990

@egotechnology

WWW.EGOTECHNOLOGY.CO.UK