

RENEW U

GDPR Policy

GDPR Policy

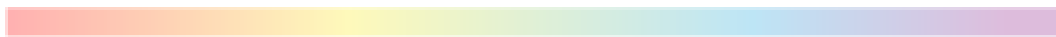
INTRODUCTION

This Policy sets out the obligations of Company, (the Company), regarding data protection and the rights of Customers, business contacts, suppliers and employees (data subjects) in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (GDPR).

The GDPR defines personal data as any information relating to an identified or identifiable natural person (a 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.

This Policy sets the company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by our company, our employees, agents, contractors, or other parties working on behalf of Company.

Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.



THE DATA PROTECTION PRINCIPLES

- We are committed to complying with the GDPR and the 8 data protection principles contained in Schedule 1 of the Data Protection Act. This Policy identifies the principles to which we as data controller and our approved data processors, handling and processing personal data will comply. To this end we ensure:

- Personal data will be processed lawfully, fairly, and in a transparent manner in relation to the data subject. It will not be processed unless it meets the conditions of processing in schedules 2 and 3 of the Data Protection Act (i.e. at least one of the conditions from schedule 2 is met and where relating to sensitive personal data, at least one of the conditions in schedule 3 is also met).

Principle 1 - Fair and lawful.

- Personal data will be 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 will not be considered to be incompatible with the initial purposes.

Principle 2 - Purposes.

- Personal data will be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Principle 3 - Adequacy.

- Personal data will be accurate and, where necessary, kept up to date. We will take reasonable steps to ensure that personal data is inaccurate, having regard to the purposes for which it is processed and that it is erased or rectified without delay.

Principle 4 - Accuracy.

- Personal data, in a form which permits identification of data subjects, will not be kept for any longer than is necessary for the purposes for which the personal data is 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 GDPR in order to safeguard the rights and freedoms of the data subject.

Principle 5 – Retention.

- Personal data will be processed in accordance with the rights of data subjects under this Act.

Principle 6 – Rights.

- Organisation and technical measures are in place that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.

Principle 7 – Security.

- Personal data will not be transferred to a country or territory outside the European Economic Area (EEA) unless we can confirm that the country or territory can ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Principle 8 – International.

THE RIGHTS OF DATA SUBJECTS

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure (also known as “the right to be forgotten”);
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights with respect to automated decision-making and profiling.

LAWFUL, FAIR, AND TRANSPARENT DATA PROCESSING

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data will be lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- 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 data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

SPECIFIED, EXPLICIT, AND LEGITIMATE PURPOSES

Company collects and processes the personal data set out within this Policy which equates to personal data collected directly from data subjects. Company only collects, processes, and holds personal data for the specific purposes set out in this Policy (or for other purposes expressly permitted by the GDPR).

Data subjects are kept informed at all times of the purpose or purposes for which Company uses their personal data. Please refer to information within keeping data subjects informed section of this policy.

ADEQUATE, RELEVANT, AND LIMITED DATA PROCESSING

Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

ACCURACY OF DATA AND KEEPING DATA UP-TO-DATE

Company will ensure that all personal data collected, processed, and held is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as detailed below in a separate section.

The accuracy of personal data will be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

DATA RETENTION

Company will not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details of Company's approach to data retention, including retention periods for specific personal data types held by Company, please refer to our Data Retention Policy.

SECURE PROCESSING

Company will ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures taken are provided later in this Policy.

TRANSFERRING PERSONAL DATA

Company will verify all destinations where there is a requirement to transfer personal data to ensure that the country or territory is within the EEA. Where we determine that the personal data is to be transferred out with the EEA, we will ensure that there is sufficient level of protection for the rights and freedoms of data beforehand. No personal data will be transferred unless assurances can be gained.

ACCOUNTABILITY AND RECORD-KEEPING

Company, the IT & Technical Co-ordinator will be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation. We will keep written internal records of all personal data collection, holding, and processing, which will incorporate the following information:

- The name and details of the Company and any applicable third-party data processors;
- The purposes for which Company collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by Company, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by Company (please refer to our separate Data Retention Policy); and
- Detailed descriptions of all technical and organisational measures taken by Company to ensure the security of personal data.

DATA PROTECTION IMPACT ASSESSMENTS

Company will carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

Data Protection Impact Assessments will be overseen by Company and will address the following:

- The type(s) of personal data that will be collected, held, and processed;
- The purpose(s) for which personal data is to be used;
- Company's objectives;
- How personal data is to be used;
- The parties (internal and/or external) who are to be consulted;
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- Risks posed to data subjects;
- Risks posed both within and to Company; and
- Proposed measures to minimise and handle identified risks.

KEEPING DATA SUBJECTS INFORMED

Company will provide the information to every data subject. Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection. Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

- If the personal data is used to communicate with the data subject, we will when the first communication is made; or
- If the personal data is to be transferred to another party, before that transfer is made; or
- As soon as reasonably possible and in any event not more than one month after the personal data is obtained. The following information will be provided:

THE FOLLOWING INFORMATION WILL BE PROVIDED:

- Details of the Company;
- The purpose(s) for which the personal data is being collected and will be processed) and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which Company is justifying its collection and processing of the personal data;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, details of those parties;
- Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place.
- Details of data retention;
- Details of the data subject's rights under the GDPR;
- Details of the data subject's right to withdraw their consent to Company's processing of their personal data at any time;
- Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

DATA SUBJECT ACCESS

Data subjects may make subject access requests (“SARs”) at any time to find out more about the personal data which Company holds about them, what it is doing with that personal data, and why. Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to, Company, IT & Technical Co-ordinator.

Responses to SARs will normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject will be informed. Company does not charge a fee for the handling of normal SARs. Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

RECTIFICATION OF PERSONAL DATA

Data subjects have the right to require Company to rectify any of their personal data that is inaccurate or incomplete. Company will rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject will be informed. In the event that any affected personal data has been disclosed to third parties, those parties will be informed of any rectification that must be made to that personal data.

ERASURE OF PERSONAL DATA

Data subjects have the right to request that Company erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to Company holding and processing their personal data;
- The data subject objects to Company holding and processing their personal data (and there is no overriding legitimate interest to allow Company to continue doing so) (see the Objections to Personal Data Processing section of this Policy for further details concerning the right to object);
- The personal data has been processed unlawfully;
- The personal data needs to be erased in order for Company to comply with a particular legal obligation.

Unless Company has reasonable grounds to refuse to erase personal data, all requests for erasure will be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject will be informed. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties will be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

RESTRICTION OF PERSONAL DATA PROCESSING

Data subjects may request that Company ceases processing the personal data it holds about them. If a data subject makes such a request, we will retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties will be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

OBJECTIONS TO PERSONAL DATA PROCESSING

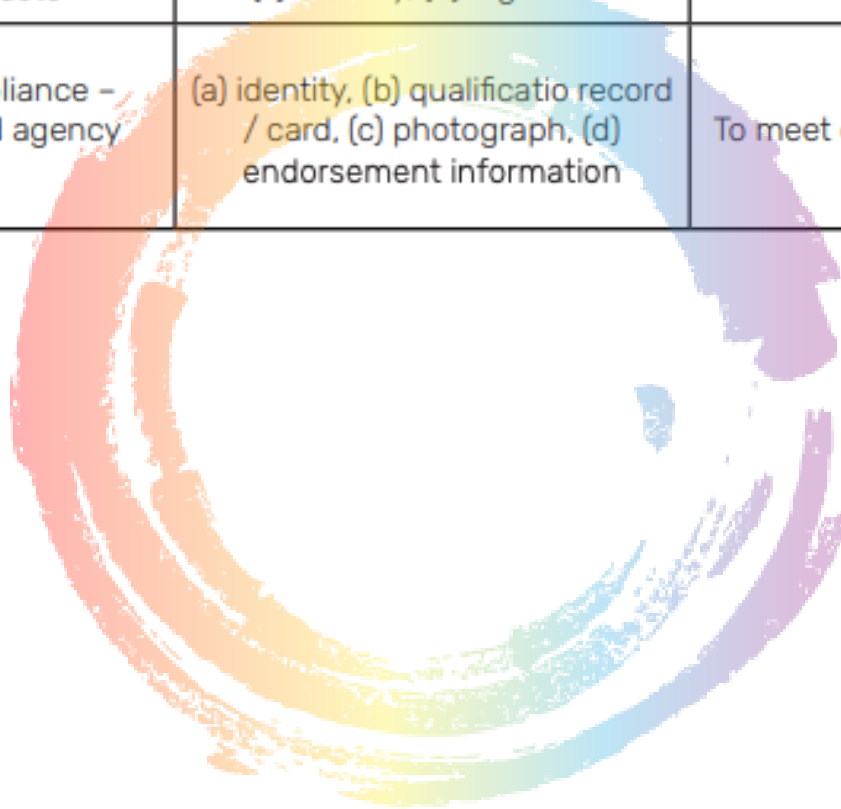
Data subjects have the right to object to Company processing their personal data based on legitimate interests, direct marketing (including profiling).

Where a data subject objects to Company processing their personal data based on its legitimate interests, we will cease such processing immediately, unless it can be demonstrated that our legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims. Where a data subject objects to Company processing their personal data for direct marketing purposes, we will cease such processing immediately.

PERSONAL DATA COLLECTED, HELD, AND PROCESSED

There is a separate policy (The Employee Privacy Notice), which identifies personal data collected, held, and processed by Company for employees and one for potential employees (Applicants Privacy Policy), therefore this section only details suppliers and customers (for details of data retention, please refer to Total Recycling Services Data Retention Policy):

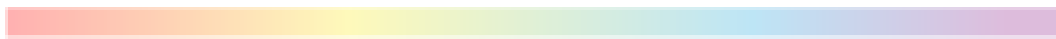
Purpose / Activity	Type of Data	Lawful basis for processing including basis of legitimate interest
To register a new customer	(a) Identity – first name, surname, (b) Contact – email address	Performance of a contract
To make a sales transaction	Bank details	Performance of a contract (only if sole trader using own name for company)
Movement of waste	(a) Identity, (b) Signature	Legal obligation
Competence compliance – sub-contractor and agency workers	(a) identity, (b) qualificatio record / card, (c) photograph, (d) endorsement information	To meet contractual obligations



DATA SECURITY – TRANSFERRING PERSONAL DATA AND COMMUNICATIONS

Company will ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- All emails containing personal data will be encrypted; All emails containing personal data will be marked “confidential”;
- Personal data will be transmitted over secure networks only; transmission over unsecured networks will not be permitted in any circumstances;
- Personal data will not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data, not already in the public domain or where lawful basis exists, contained in the body of an email, whether sent or received, will be copied from the body of that email and stored securely. The email itself will be deleted. All temporary files associated therewith will also be deleted subject to the same criteria (i.e. information not already widely available in the public domain or lawful basis not obtained);
- Where personal data is sent by facsimile transmission the recipient will be informed in advance of the transmission so that they can prepare for its arrival by waiting by the fax machine to receive the data;
- Where personal data is to be transferred in hardcopy form it will be passed directly to the recipient or sent using a tracked or registered postal service; and
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic media will be transferred in a suitable container marked “confidential”.
- A Data Processing Agreement will be implemented and signed where 3rd party processors are utilised or are required to process personal and sensitive data.




DATA SECURITY - STORAGE

Company will ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data will be stored securely using passwords and data encryption;
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media will be stored securely in a locked box, drawer, cabinet, or similar;
- All personal data stored electronically will be backed up frequently with backups. All backups should be encrypted;
- No personal data will be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to Company or otherwise without the formal written approval of Name Here, Managing Director and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
- No personal data will be transferred to any device personally belonging to an employee and personal data will only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to Company that all suitable technical and organisational measures have been taken).

DATA SECURITY - DISPOSAL

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it will be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to Company's Data Retention Policy.



DATA SECURITY – USE OF PERSONAL DATA

Company will ensure that the following measures are taken with respect to the use of personal data:

- No personal data will be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of Company requires access to any personal data that they do not already have access to, such access should be formally requested from Natalie Matharu;
 - No personal data will be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of Company or not, without the authorisation of Natalie Matharu;
 - Personal data will be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
 - If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user will lock the computer and screen before leaving it;
- and
- Where personal data held by Company is used for marketing purposes, it will be the responsibility of Natalie Matharu to ensure that there is a legitimate interest or appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third party service such as the TPS.

DATA SECURITY – IT SECURITY

Company will ensure that the following measures are taken with respect to IT and information security:

- All passwords used to protect personal data will be changed regularly and will not use words or phrases that can be easily guessed or otherwise compromised. All passwords will contain a combination of uppercase and lowercase letters, numbers, and symbols;
- Under no circumstances will any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method;
- All software (including, but not limited to, applications and operating systems) will be kept up-to-date; and
- No software may be installed on any Company-owned computer or device without the prior approval of the Managing Director.

ORGANISATIONAL MEASURES

Company will ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of Company will be made fully aware of both their individual responsibilities and Company's responsibilities under the GDPR and under this Policy, and will be provided with a copy of this Policy;
- Only employees, agents, sub-contractors, or other parties working on behalf of Company that need access to, and use of, personal data in order to carry out their assigned duties correctly will have access to personal data held by Company;
- All employees, agents, contractors, or other parties working on behalf of Company handling personal data will be appropriately trained to do so;
- All employees, agents, contractors, or other parties working on behalf of Company handling personal data will be appropriately supervised;
- All employees, agents, contractors, or other parties working on behalf of Company handling personal data will be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- Methods of collecting, holding, and processing personal data will be regularly evaluated and reviewed;
- All personal data held by Company will be reviewed periodically, as set out in Company's Data Retention Policy;
- The performance of those employees, agents, contractors, or other parties working on behalf of Company handling personal data will be regularly evaluated and reviewed;
- All employees, agents, contractors, or other parties working on behalf of Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
- All agents, contractors, or other parties working on behalf of Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Company arising out of this Policy and the GDPR; and
- Where any agent, contractor or other party working on behalf of Company handling personal data fails in their obligations under this Policy that party will indemnify and hold harmless Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

The transfer of personal data to a country outside of the EEA will take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- The transfer is made with the informed consent of the relevant data subject(s);
- The transfer is necessary for the performance of a contract between the data subject and Company (or for pre-contractual steps taken at the request of the data subject);
- The transfer is necessary for important public interest reasons;
- The transfer is necessary for the conduct of legal claims;
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register

DATA BREACH NOTIFICATION

All personal data breaches must be reported immediately to Company, the IT & Technical Coordinator.

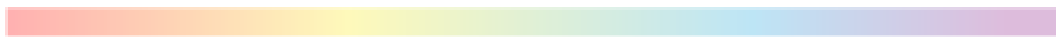
If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the

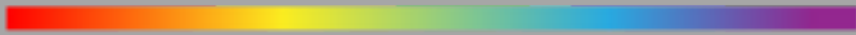
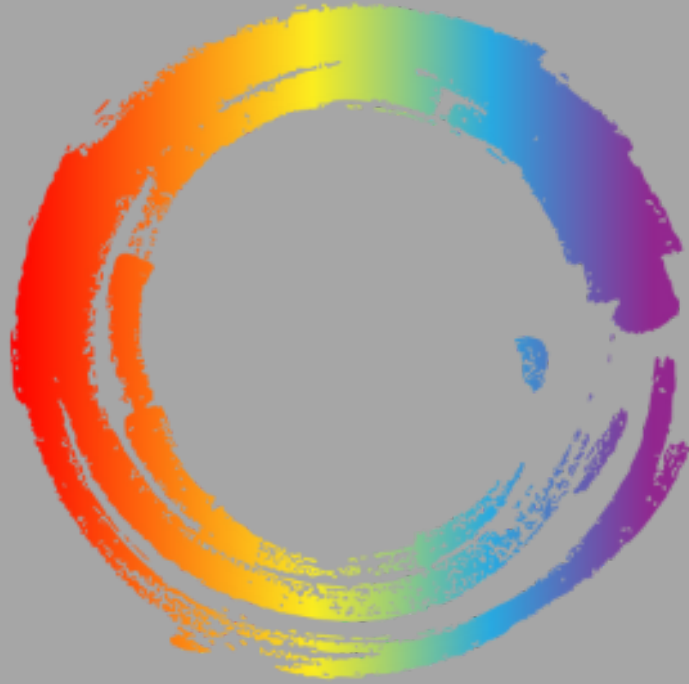
IT Administrator will ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications will include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of Company's data protection officer (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by Company to
- address the breach including, where appropriate, measures to mitigate its possible adverse effects.





RENEW U

GDPR Policy