DATA PROTECTION POLICY

APPROVAL

Approved by the Executive Committee of Renewable World ("RW") on 7th March 2022.
Date of next review: 7th March 2024.

Renewable World is fully committed to complying with the requirements of the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) and, where applicable, the EU General Data Protection Regulation (EU GDPR)[1].

INTRODUCTION

This policy sets out the principles which Renewable World (RW) intends to apply to the processing of personal data.

This policy applies to all personnel of RW. In this policy, "personnel" includes but is not limited to all Trustees, employees, officers, consultants, contractors, volunteers, agency workers and anyone else working on behalf of RW – i.e. anyone who is likely to come into contact with personal data which is being processed by RW.

Compliance by personnel with this policy is essential not only because of the damage that could be caused to personnel and/or third parties in the event of a data protection breach and the reputational damage that could be caused to RW but also because RW could be liable to pay a substantial fine.

Accordingly, all personnel have a personal responsibility to ensure compliance with this policy (and related policies) and to handle all personal data consistently with the principles relating to the processing of personal data set out below. Managers and other senior individuals are expected to monitor and enforce compliance with this policy.

Any breach of this policy will be treated very seriously and may result in action under RW's disciplinary procedure. If any member of personnel becomes aware that the policy is being breached in any way, this should be reported to the Global Finance and Administration Manager.

This policy does not create any contractual rights and does not form part of any contractual relationship between RW and any of its personnel or any third party. RW reserves the right to amend this policy at any time. Any changes will be notified to personnel by email.

TECHNICAL TERMS

A number of terms applied in this policy are defined in the applicable legislation. Understanding the meaning of such terms may assist personnel to comply with this policy, and their definitions are therefore set out at the end of the policy.

[1] https://www.itgovernance.co.uk/dpa-2018

OTHER RELEVANT INFORMATION

This policy should not be read in isolation. There are various other documents which personnel must read in order to understand their rights and obligations in relation to personal data. These are set out below and can be found on Dropbox [\Dropbox (Renewable World)\RW Human Resources (HR)\HR policies]:

- Privacy Policy
- Data Breach Notification Policy
- Data Retention Policy

OVERALL RESPONSIBILITY FOR DATA PROTECTION WITHIN RW

The person with overall responsibility for data protection within RW and for upholding and enforcing the terms of this policy is the Global Finance and Administration Manager. Personnel should contact the Global Finance and Administration Manager in relation to any data protection issues. In particular, any member of personnel should contact the Global Finance and Administration Manager immediately if he or she becomes aware:

- that anyone within RW is not complying or may not be complying with any part of this policy;
- that RW is engaging in a new processing activity or there has been a change to existing processing activities;
- of an actual or suspected personal data breach (in which case that member of personnel should also refer to the Data Breach Notification Policy for further information [found on \Dropbox (Renewable World)\RW Human Resources (HR)\HR policies\Data protection], or
- that a subject access request or other request to enforce rights available to data subjects under data protection legislation has been received by RW.

For the avoidance of doubt, the individual with overall responsibility for data protection within RW and for upholding and enforcing the terms of this policy is not a formal Data Protection Officer within the meaning of that phrase in applicable legislation.

ACCOUNTABILITY

RW is responsible for ensuring compliance with the principles relating to the processing of personal data (which are set out below) and must also be able to demonstrate that it is compliant. It aims to do so by:

- appointing an individual with overall responsibility for data protection within RW and for upholding and enforcing the terms of this policy;
- drafting, maintaining and implementing various policies and procedures relating to personal data processing;
- arranging regular, mandatory training for its members of personnel in relation to data protection, as required, so that they understand their obligations and can work with RW to ensure that personal data is processed fairly and lawfully;
- maintaining records of its processing activities;
- conducting due diligence on services providers who process personal data on RW's behalf, including taking reasonable steps to ensure those providers are capable of complying with the data protection principles, any data subject requests that RW may receive and any obligations under data protection legislation which RW may delegate to such service providers; and
- carrying out data protection impact assessments (DPIAs) when using new technologies or undertaking processing which is likely to result in a high risk to the rights and freedoms of

individuals to help RW identify the most effective way to comply with its data protection obligations and to meet the expectations of privacy of its personnel and clients.

THE DATA PROTECTION PRINCIPLES

In order to understand the obligations owed by both RW and its personnel in relation to the processing of personal data, personnel need to be aware of the seven principles that underpin the lawful processing of personal data. These are set out below.

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency);
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation);
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);
4. accurate and, where necessary, kept up to date (accuracy);
5. kept in a form which permits identification of subjects for no longer than is necessary for the purposes for which the personal data is processed (storage limitation);
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or lawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures (integrity, confidentiality and security).; and
7. the controller shall be responsible for and be able to demonstrate compliance with the data protection principles listed above (accountability).

The steps adopted by RW to achieve compliance with each of these principles are set out below. All personnel are required to adhere to the steps set out below.

1. LAWFUL, FAIR AND TRANSPARENT PROCESSING

For personal data to be processed lawfully, there must be a lawful basis for processing it. RW processes data because it is necessary:

- for the performance of contracts; or
- for compliance with any legal obligation to which it is subject; or
- for the purposes of the legitimate interests pursued by RW or 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 the data subject.

In addition, RW may in certain circumstances rely on consent to process certain categories of personal data. For consent to be valid, it must be specific, informed, unambiguous and freely-given and the data subject has the right to withdraw that consent at any time (and must be advised of the right to do so). Where RW intends to rely on consent to process any particular category of personal data, this must be authorised by the Global Finance and Administration Manager.

RW aims to be as transparent as possible in its processing of personal data and to ensure that data subjects are aware: that their personal data is being processed; which categories of personal data is being processed (including special category data where applicable) and on what lawful basis; which third parties receive it;

how long it is retained and that they have certain rights under the applicable legislation. All this information is contained in RW's Privacy Policy. This can be found on our website or on Dropbox [\Dropbox (Renewable World)\RW Human Resources (HR) (1)\HR policies\Privacy Policy].

2. PURPOSE LIMITATION

RW aims only to process personal data for the legitimate purposes for which such data was collected, such purposes being specified in the applicable privacy notice. In particular, RW aims to limit the purposes for which it collects any special category data – for example, personal data in relation to sickness absence are collected in order to monitor attendance, process sick pay, to establish entitlement to any applicable benefits, and so that RW can comply with any obligations under the Equality Act 2010.

Should it no longer be necessary to process personal data for the purpose (or purposes) for which it was originally collected, it may be necessary to delete it in accordance with RW's Data Retention Policy [\Dropbox (Renewable World)\RW Human Resources (HR)\HR policies]. Alternatively, if the purpose for which the personal data is being processed has changed but processing is still legitimate, data subjects should be informed as soon as possible via an updated privacy notice. If an employee becomes aware that personal data is being processed for a reason other than that for which it was originally collected, s/he should notify the Global Finance and Administration Manager.

3. DATA MINIMISATION

RW aims to limit its processing of personal data to circumstances where such processing is adequate, relevant and necessary for the purposes for which such data is being processed.

In particular, RW aims to limit its processing of special category data. Special category data in relation to personnel will only be processed by the HR department and will be accessed only by individuals within the Finance and Corporate Services team and managers, as appropriate.

Personnel should only process personal data as is necessary in order to carry out their duties for RW and should avoid processing or disseminating personal data unnecessarily. For example, individual personnel members should consider whether it is necessary:

- to retain multiple drafts (rather than the final version) of a document;
- for multiple personnel (rather than a single personnel member) to retain a copy of a particular document (or if only one person needs to keep it);
- to retain hard copies of a document if there is a soft copy;
- to copy multiple individuals on emails which contain personal data (in particular special category data); and
- to use "reply all" on emails containing such personal data.

Personnel should not process any personal data on RW's systems that are unrelated to work. For example, personnel should not:

- send personal emails containing personal data from their work email account; or
- store personal data relating to their contacts on their work Outlook folders or diary.

4. ACCURACY

RW takes steps to ensure that the personal data which it processes are kept accurate and up-to-date. Personnel are asked to notify Finance and Corporate Services team if any of their contact or other personal details need to be updated.

Any member of personnel who is processing personal data on behalf of RW is responsible for ensuring that such personal data is accurate at the point of collection, and that it is reviewed on a regular and systematic basis to ensure that it remains up-to-date.

If a member of personnel becomes aware that any personal data processed by RW is inaccurate – whether his/her own, that of a colleague or that of a client or other third party, that member of personnel must either ensure that it is corrected; or should contact the appropriate person to make the necessary correction; or should contact the Global Finance and Administration Manager if it may be appropriate for it to be deleted.

5. STORAGE LIMITATION

A copy of RW's Data Retention Policy can be found at \Dropbox (Renewable World)\RW Human Resources (HR)\HR policies\Data protection. Personnel are required to familiarise themselves with any relevant retention periods and to ensure that they adhere to them in respect of any personal data for which they are responsible. After the relevant retention period has expired, personal data should be permanently deleted or anonymized in accordance with the terms of the Data Retention Policy.

6. INTEGRITY, CONFIDENTIALITY AND SECURITY

RW has put appropriate security in place to protect against data breaches. Those security measures include: lockable offices; personal data kept in locked cupboards/filing cabinets; methods of disposal; use of designated drivers/servers and storage facilities; and use of approved security software. Where personal data, and in particular special category data is transferred to a third party, RW has satisfied itself that similar security measures are in place.

RW expects each personnel member to use his or her best efforts to ensure that personal data is processed lawfully and securely. There are some simple steps which personnel can take to help RW achieve this:

- operate a "clear desk" policy so that hard copy personal data is not left lying around;
- documents containing personal data, and in particular those containing special category data, should be stored securely. If they are in hard copy form they should be kept in a locked filing cabinet. Soft copy documents should also be stored securely by, for example, password protecting them or storing them in a folder with limited access;
- computers and handheld devices used for work purposes should be password protected with a sufficiently strong password [see RW's IT Policy for further details]. Passwords should never be shared. When a computer is left unattended in the office, it should always be locked. A work computer or handheld device should never be left unattended outside the office;
- personal data should be saved only to designated drives and servers and should be uploaded only to an approved storage system. Personnel must not save personal data locally or send it to their personal email addresses;
- personal data, and in particular special category data, should not be taken outside the office where this can be avoided. If this is necessary, such data should be treated with care and, if possible, password protected or encrypted soft copies should be taken outside the office rather than hard copies;

- if disposing of hard copy documents containing personal data, these should be shredded securely;
- particular care should be taken when writing emails and documents which may contain personal data. Personnel should consider whether it is necessary to include personal data (in particular if it is special category data). If so, personnel should ensure that the content is appropriate and that the contents of such communication is suitable to be shared with the data subject; and
- particular care should also be taken, when writing an email which contains personal data, to ensure that it is only sent to appropriate recipients. Further care should be taken where recipients' names have been auto-filled.

7. ACCOUNTABILITY

RW takes responsibility for what we do with personal data and has taken steps to ensure that we are able to demonstrate compliance with the data protection principles listed above. We have appropriate measures and records in place to be able to demonstrate our compliance. These include:

- ensuring all personnel comply with this Policy;
- maintaining relevant documentation on processing activities and other records;
- providing all personnel who deal with personal data training relating to data protection;
- ensuring that all personnel notify the Global Finance and Administration Manager if they have any areas of concern about data protection compliance or risks that they consider are not being adequately addressed; and
- ensuring we keep full and accurate records of all our data processing activities.

SPECIAL CATEGORY DATA

RW collects and processes certain categories of special category data for its personnel. Further details of the types of special category data RW processes and its lawful bases for doing so, are set out in the applicable privacy notice. The steps taken by RW to ensure that such special category data is processed in compliance with the data protection principles are set out above.

The retention periods for the categories of special category data processed by RW are set out in RW's Data Retention Policy [\Dropbox (Renewable World)\RW Human Resources (HR)\HR policies].

INTERNATIONAL TRANSFERS

There are restrictions on RW's ability to transfer personal data outside the European Economic Area (EEA) to ensure that the level of protection afforded by EU data protection legislation is not undermined.

RW may transfer personal data outside the EEA. Further details in relation to this will be set out in the Privacy Policy.

Any member of personnel who is required to transfer data out of the EEA should be clear that there is authorisation to do so. If in any doubt, the matter should be referred to a line manager and/or the Global Finance and Administration Manager.

SHARING PERSONAL DATA

RW is generally not permitted to share personal data with a third party unless certain safeguards and contractual arrangements are in place so that it can be satisfied that third parties are processing personal data in compliance with data protection legislation.

Members of personnel should not share personal data with third parties where there is no business need to do so.

Any member of personnel who is required to share personal data with a third party should be clear that there is authorisation to do so. If in any doubt, the matter should be referred to a line manager and/or the Global Finance and Administration Manager.

REPORTING A PERSONAL DATA BREACH

In the event of a personal data breach there may be an obligation on RW to report such a breach to the Information Commissioner's Office (ICO) or any individuals affected by the breach within 72 hours. Please refer to RW's Data Breach Notification Policy [Dropbox (Renewable World)\RW Human Resources (HR)\HR policies] for further details.

DATA SUBJECTS RIGHTS

Data subjects have various rights under the applicable data protection legislation and these are set out in Renewable World's Privacy Notice. The UK GDPR provides the following rights for individuals:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object; and
8. Rights in relation to automated decision making and profiling.

Further information is also available from the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/.

FURTHER INFORMATION

RW promotes transparency in its processing of personal data. If any member of personnel has any questions about this policy, please contact the Global Finance and Administration Manager [Janaki Jayasuriya, Janaki.Jayasuriya@renewable-world.org].

DEFINED TERMS

Controller: the entity which alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this policy, the Controller is RW.

Personal data: 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.

Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Processing: 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.

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

Special Category Data: 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 purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

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