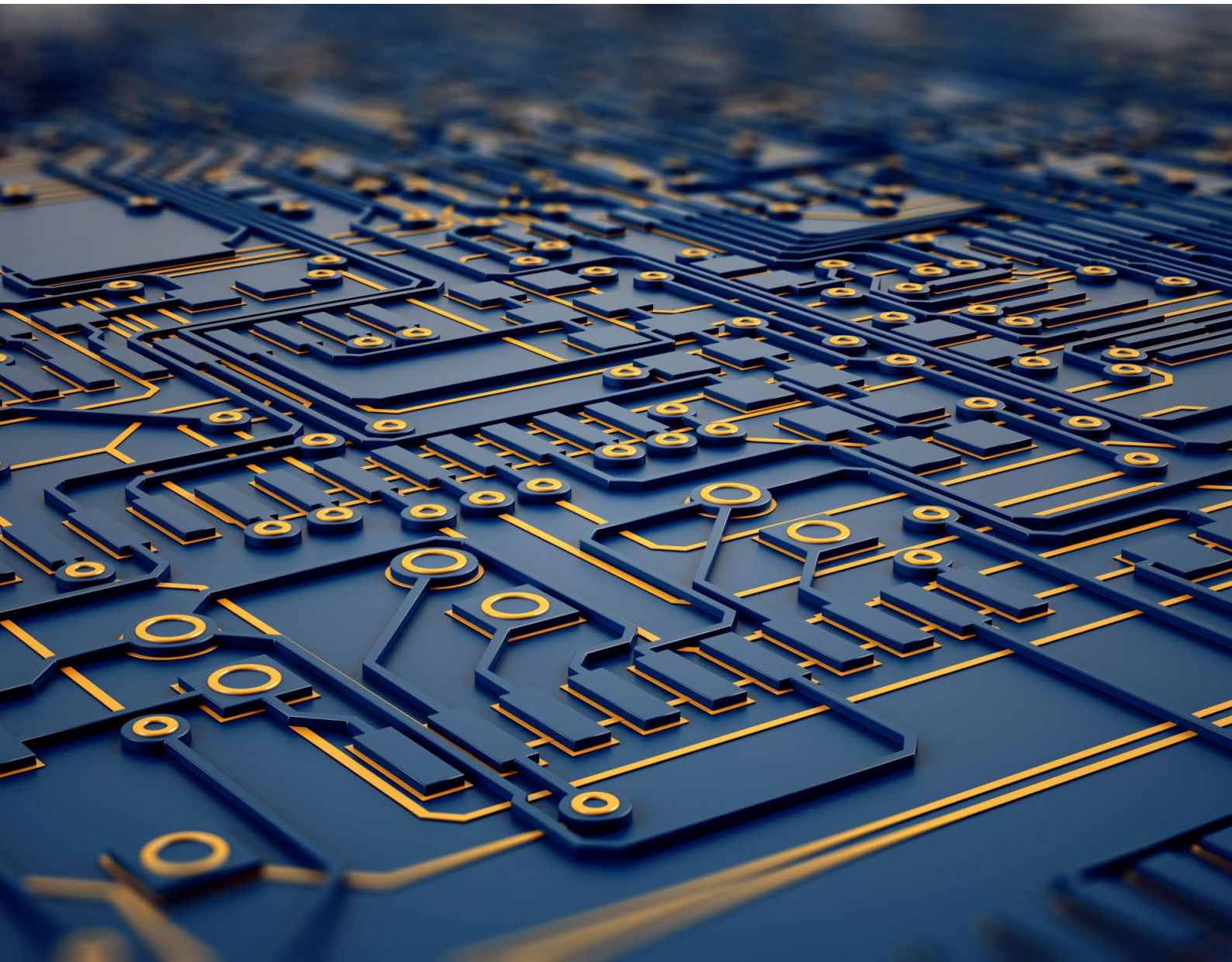
EarthCheck Data Protection Policy

Policy/Version # 2018.0001/002

Effective Date: 24/09/2018



CONTENTS

Date	Description	Author	Approver
24/09/2018	Initial Approval and Review	Tarjani Pilkington	Glenn Jones
23/11/2021	Policy Review	Tarjani Pilkington	Stewart Moore

DEFINITIONS

Consent	Refers to any freely given, specific, informed and unambiguous indication of the data subject's wishes, by a statement or by a clear affirmative action, to signify agreement to the processing of personal data relating to him or her.
Data Controller	Refers to 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.
Data Processor	Refers to an entity that handles data on behalf of the data controller.
Data Processing	Refers to the processes, or actions, performed on personal data or on sets of personal data. These actions may or may not be by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, restriction, erasure or destruction of data.
Data Subject	Refers to an individual whose personal data is being collected, held or processed that can be identified directly or indirectly by the data being collected.
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'). Identifiable personal data may include: 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.
Sensitive Personal Data	Refers to data that is revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
Third Party	Refers to 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.

1 POLICY STATEMENT

1.1 Data Protection Policy Objective

In this digital age of data collection, protection of this information is a pivotal part of business relationships. As a driving force in supporting sustainability and corporate social responsibility, EarthCheck recognises the importance of data security, and is committed to maintaining compliance with international standards on data protection.

This data protection policy provides a framework on international data handling for the EarthCheck community. The policy is based on globally accepted principals on data protection, adhering to privacy principles within Australia and the EU General Data Protection Regulations (GDPR). This policy is to act as a guideline for EarthCheck practices pertaining to information on our new and existing customers, business partners and employees.

1.2 Scope of the Data Protection Policy

The contents of this data protection policy are instructions on the processing of data by all internal employees, EarthCheck interns and external contractors. While this policy focuses on the processing of digital data, information that is kept in a physical form is also considered.

The Data Protection Policy focuses on the processing of personal data. Data collected by EarthCheck is primarily the data of legal entities, however it is recognised that personal data will be provided by businesses at times. Personal data is also relevant within the scope of employee data that is held regarding the period of employment with EarthCheck.

The latest version of the Data Protection Policy can be accessed with the data privacy information at EarthCheck's website: www.earthcheck.org

2 SCOPE OF EARTHCHECK DATA COLLECTION

Data collected by EarthCheck primarily focuses on sustainability metrics to enhance operational performance and reduce the organisations environmental impact. However, EarthCheck acknowledges that during the collection of such data individual users may provide personal information. This policy considers personal data acquired by EarthCheck within the context of EarthCheck customers and partners and within the context of employment.

2.1 Customer and Partner Data

While this list is not exhaustive, personal data for customers/partners is collected in the following instances:

- When registering for our products;
- When registering as a subscriber to one of our newsletters;
- Voluntarily at certain other points, such as contests or surveys;

- Tracking information, which is automatically collected about all visitors to our sites.

Examples of Customer and Partner personal data:

- Your Name
- Job Title & Position in organisation
- Phone Number/Skype Details
- Email Address
- Location
- IP Address

2.2 Employee Data

While this list is not exhaustive, personal data for employees is collected in the following instances:

- During the recruitment process
- Throughout initial employment onboarding
- As employee details

Examples of Customer and Partner personal data:

- Name
- Job Title & Position in organisation
- Phone Number
- Personal Email Address
- Work Email Address
- Home Address
- Banking Details
- Superannuation Details
- Tax Information
- Photographic records for identification

3 RIGHTS OF THE DATA SUBJECT

Data protection extends beyond the processing of personal data of a data subject, however the GDPR grants people specific data subject rights that they can exercise under particular conditions. Key data subject rights that should be considered when EarthCheck is processing data include:

1. **The right to be informed**
   The data subject has the right to clear and transparent communication regarding the purposes for which their data will be processed.
2. **The right of access**
   The data subject may request information on which personal data relating to him/her has been stored, how the data was collected, and for what purpose. Organisations must respond to this request within 30 days and provide individuals access to the data they hold on to them without any charge.
3. **The right of rectification**
   If personal data is incorrect, the data subject has the right to have it be corrected. Upon correction, EarthCheck is required to send the correction to third parties with whom the data is shared.
4. **The right to erasure**
   The data subject may request their data to be deleted if it is no longer required for the purpose which it was collected if the data subject withdraws consent or if the data processing has no legal basis.
5. **The right to restrict processing**

The data subject has the right to restrict how their data is processed. This may provide an alternative to having the data erased whereby it can be stored but not processed. This is also an alternative, if a complaint or further right has been requested and is still being processed.

6. **The right to data portability**
   Data subjects have a right to receive a copy of their personal data in a commonly used, electronic format that supports re-use.
7. **The right to object**
   The data subject has a right to object to his/her data being processed. The data subject can object to the processing of his or her data for purposes of advertising or market/opinion research.
8. **The right and access to raise a complaint**
   The data subject shall have the ability to raise a complaint to EarthCheck regarding data concerns, and if these are not addressed the ability to escalate this to a supervisory authority.

These rights are a reflection of articles 12 – 22 in the EU General Data Protection Regulations. Further details on the data subject rights can be found in Chapter 3 of the General Data Protection Regulation.

4 PRINCIPLES FOR PROCESSING PERSONAL DATA

The following principles are grounding elements of data regulations and have been considered as founding principles for the processing of personal data within EarthCheck.

1. **Lawful and Fair Processing**
   Any processing of data, particularly personal data, should be lawful and fair. It should be transparent to the data subject that data concerning them is collected, used, consulted or otherwise processed and to what extent the personal data will be processed.
2. **Transparency**
   The principle of transparency requires that the data subject be informed as to how their data is being handled. When the data is collected, the data subject must either be aware of, or informed of the purpose of data and if the data will be transmitted to any third parties. Communication that is addressed to the public or to the data subject must be concise, easily accessible and easy to understand.
3. **Purpose Limitation**
   Processing of data, particularly personal data, can be only processed for the purpose that was initially declared at the point of collection. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.
4. **Data Minimisation**
   Before processing personal data, it must be determined whether and to what extent the processing of personal data is necessary, in order to achieve the purpose for which it is undertaken.
5. **Factual Accuracy of Data**
   The storage of personal data that is stored on file must be correct, complete, and – where required – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data is corrected/updated when advice of a change is provided.
6. **Data Subject Rights**
   Data subjects should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

7. **Confidentiality and Data Security**
   Data that is processed and stored, particularly personal data, is subject to data secrecy. It must be treated as in a manner that ensures it is secured with suitable organizational and technical measures to prevent unauthorized access, accidental loss, modification or destruction.

These principles reflect article 5 in the EU General Data Protection Regulations*, additional details can be found in* Recital 39 *of the GDPR.*

5 DATA PROCESSING REQUIREMENTS

Within the scope of EarthCheck operational practices, personal data is considered as customer and partner data, and employee data. The following requirements are to be adhered to during the collection, processing and storage of personal data.

5.1 Customer and Partner Data

5.1.1 Data processing for advertising purposes

If the data subject contacts EarthCheck as a product/service enquiry, data processing to meet this request is permitted. EarthCheck does not require users to become members of EarthCheck in order to have access to our free email newsletters, however individuals will have to supply their email address and provide us with some additional information as required.

Processing of personal data that is consistent with the purpose for which the data was originally collected, can be processed for advertising purposes or market and opinion research. The data subject should be informed about the use of his/her data for advertising purposes. If the data subject refuses the use of his/her data for advertising purposes, it can no longer be used for these purposes. EarthCheck may disclose all the information collected as described above to other companies such as direct marketers to perform marketing services on our behalf, or to financial institutions, such as banks, insurance companies and securities broker-dealers, with whom have joint marketing agreements are made.

5.1.2 Data processing for a relationship

Data processing is required for the forming new contractual relationships and to maintain or terminate existing contracts. This processing may also be completed by third party services for EarthCheck if this is related to the contractual purpose. During the contract initiation phase, personal data may be required for processing with the prospecting business details, to prepare quotes or to fulfil other requests of the prospect that relate to contract conclusion.

5.1.3 Consent to data processing

Processing of data requires consent of the data subject. The consent must be documented in writing or electronically for the purposes of being able to demonstrate that consent was obtained. Verbal

consent may be given via telephone where the call is recorded. The data subject must also have the ability to withdraw his or her consent with the same ease of the initial consent.

5.1.4 User data and internet

If personal data is collected, processed and used on websites or in apps, the data subjects must be informed of this in a privacy statement or other electronic means on the platform, and if applicable, information about cookies. The privacy statement and any cookie information must be consistently available for the data subjects and provide options for the user to opt out.

5.2 Employee Data

5.2.1 Data processing for the employment relationship

When initiating an employment relationship, the applicants' personal data can be processed. During the period of employment, personal data can be processed if needed to initiate, carry out and terminate the employment agreement. It may be necessary during the application procedure to collect information on an applicant from a third party, to commence the recruitment process. Personal data can also be processed during the planning of organisational work, equality and diversity in the workplace and health and safety in the workplace on an individual or collective.

5.2.2 Consent to data processing

Consent for the processing of the employee data should be obtained during the initial recruitment process, and with the initial agreement signed on commencing employment.

5.2.3 Telecommunications and internet

Telephone equipment, e-mail addresses, intranet and internet are a company resource and provided to employees by the company primarily for work-related purposes. They can be used within the applicable legal regulations and internal company policies.

6 THIRD PARTY DATA PROCESSING

Third party data processing means that a provider is hired to process data, without being assigned responsibility for the business process. In this case, the third-party can process personal data only as per the instructions from EarthCheck. The following requirements must be complied with, and the connected department must ensure that they are met:

1. The contractual standards for data protection provided by EarthCheck must be followed.
2. EarthCheck must be confident that the provider will comply with the contracted duties.
3. Depending on the risk of data processing, the reviews should be repeated on a regular basis during the term of the contract.

7 CONFIDENTIALITY OF PROCESSING

Personal data is subject to confidentiality in the collection, processing, or use of such data by employees. EarthCheck limits access to personal information to those employees whom we determine need access to that information to provide products or services. Employees should have access to personal information only as is appropriate for the type and scope of their work.

7.1 Authorisation for Disclosures

Authorisation for disclosure of personal data falls into two main categories: those likely to be at the instigation of the Data Subject, and those which are made in official investigations.

7.1.1 Instigation of Data Subject

Requests for disclosure from either a customer, partner or employee should be directly from the data subject in writing. If the request is from a party other than the data subject, consent should be gained before providing the information. This process and the response should be recorded and kept for future records.

7.1.2 Official Investigations

Requests that result from an official investigation, it may be appropriate for the Data Subject not even to be informed. Authorisation for this disclosure should be made at a senior level within your organisation. This process should be recorded and kept for future records.

8 DATA SECURITY

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. These measures should ensure that of methods of security and privacy by design are incorporated in new systems and processes.

8.1 Security measures

The EarthCheck Information Security system policies have been developed to ascertain the technologies used as threat protection and the required staff behaviours to ensure data security. These security measure in place include the use of firewalls and threat protection software, limited systems security access as per role requirements, restricted password requirements, and internet/email interactions.

8.2 Business Continuity

The EarthCheck Business Continuity Plan (BCP) is devised to deal with the impact of an event or disruption occurring to the business. The primary focus of the BCP the continuation of business processes and scheduled backups to protected data. Within the context of business continuity, the

ongoing data backups will be for both business and personal data of EarthCheck members, customers, partners, contractors or staff.

BC planning is a dynamic and iterative process, which allows for further development and adaptation as circumstances change or risks evolve. Updates to the BCP lie with the ICT team with Senior Management to review periodic updates.

9 DATA PROTECTION CONTROL

Compliance with the Data Protection Policy and the applicable data protection laws is checked with data protection audits and other controls. The performance of these controls is the responsibility of the ICT Team, the data protection coordinators and the management team. On request, the results of data protection controls will be made available to the responsible data protection authority.
Sources of non-electronic personal data (paper or otherwise) will be kept in a locked cabinet or similar locations of restricted access. Examples of such data may include employee personal records.

10 DATA BREACH INCIDENTS

A data breach is an incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed outside of the business in an unauthorised manner. All employees must inform their manager immediately about cases of suspected or confirmed breaches of this Policy or other regulations on the protection of personal data (data breach incidents). The manager responsible for the function or the unit is required to inform the responsible data protection coordinator immediately about data protection incidents.

10.1 Mandatory data breach notification

According the GDPR, data controllers must advise the relevant supervisory authority of a breach of personal data within 72 hours of becoming aware of the breach. However, if the data breach is unlikely to result in a high risk to the rights and freedoms of individuals, the notification is not mandatory. Reporting of a breach must be made to the data controller without delay (GDPR Article 33). Furthermore, if a data breach could result in a risk to the rights and freedoms of an individual, the controller must notify the individual without delay (GDPR Article 34).

Australian Privacy Act
A notifiable data breaches scheme commenced in Australia on 22 February 2018. The scheme applies to 'eligible data breaches'—where the breach is likely to result in serious harm to any of the individuals to whom the information relates. It requires APP entities to provide a statement to the Commissioner notifying of an eligible data breach as soon as practicable after the entity becomes aware of the breach. It also requires entities to notify affected individuals as soon as practicable after preparing the statement for the Commissioner. Like the GDPR, exceptions to these requirements. For more information, see **www.oaic.gov.au/ndb**

11 RESPONSIBILITIES AND SANCTIONS

Compliance with required data regulations should be addressed through this policy so that all staff aware of their shared responsibilities. Management staff are responsible for ensuring that organizational, HR, and technical measures are in place so that any data processing is carried out in accordance with data protection. Mores specific maintenance of the data policy and awareness on evolving data regulations will fall with the data protection officer. Non-compliance with required responsibilities may result in sanctions and other measures by relevant governing bodies.

11.1 Responsibilities

11.1.1 Data Protection Officer

EarthCheck will delegate an employee to be the data protection officer, who will have the following responsibilities:

- Reviewing Data Protection and related policies
- Advising other staff on potential Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Handling subject access requests
- Overseeing unusual or controversial disclosures of personal data (if the delegate is not the authorising person, they will ensure that the disclosures are authorised by appropriate managers)

11.1.2 Team/Department managers

Each team manager is responsible for ensuring that their team, has received the relevant induction training, and updates required for awareness on how to be compliant.

11.1.3 Staff & Interns

All staff/interns should be required to read, understand and accept any policies and procedures that relate to the personal data they may handle during their work.

11.2 Sanctions

Non-compliance with data regulations may result in sanctions that may result in administrative fines and negative public relations for the business.

11.2.1 GDPR Sanctions

Under the GDPR, supervisory authorities can impose administrative fines for breaches, with potential fines of up to €20 million or 4 per cent of annual worldwide turnover (GDPR Article 83(5)). Infringements that are subject to a maximum penalty include:

- the data processing principles in Articles 5, 6, 7, and 9 (including conditions for consent);

- the data subjects' rights under Articles 12 to 22 (such as rights to transparency, access rectification, right to be forgotten to personal data and right to data portability);
- the requirements relating to the transfer of personal data to a recipient in a third country or an international organisation under Articles 44 to 49;

12 STAFF TRAINING & ACCEPTANCE OF RESPONSIBILITIES

12.1 Staff Induction

All staff who have access to any kind of personal data should have their responsibilities outlined during their induction procedures. They should sign off that they have completed the induction/policy and are aware of the required responsibilities with their data engagement.

12.2 Ongoing Training

Due to the evolving nature of data regulations, new policies and new developments to existing policies will be required. Any updates should be provided to staff in ongoing training sessions, which may be provided during staff training, team meetings, or other electronic means of review. Staff should have a means to do a written or electronic sign off they have attended/reviewed the changes and understand their responsibilities.

13 POLICY REVIEW

This policy will be reviewed regularly and updated in accordance with the legislation and relevant business developments. Policy updates will be the responsibility of the data protection officer, with required authorisation from senior management.