EOH Privacy Policy

Policy Owner	Chief Risk Officer
Policy Custodian	Chief Compliance Officer
Approved by	EOH Board of Directors
Approval/Effective date	02 April 2020
Next Review Date	02 April 2022

Table of Contents

Abbreviations

ACRONYM	STANDS FOR
EOH	EOH Holdings Limited and all of its subsidiaries, affiliates and business employees (i.e. employees, directors, senior managers, executives, temporary staff members, agents, consultants, seconded, home-based, casual and agency staff, volunteers and interns), EOH service providers and EOH business associates and partners.
Data Protection Laws	Means all applicable law relating to data protection, privacy and security when processing Personal Information under the Agreement. This includes without limitation applicable international and local data protection, privacy, export or data security directives including the Electronic Communications and Transactions Act 25 of 2002, Protection of Personal Information Act 4 of 2013 and the General Data Protection Regulation.
Personal Information	Personal data is any data recorded electronically or in hard copy, that if viewed on its own, or collectively with other data, can be used to uniquely identify an individual or a legal entity.
Processing	means any operation, or set of operations, performed on Data, by any means, such as by collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction and "Processing" shall have a corresponding meaning.
GDPR	General Data Protection Regulation
POPIA	Protection of Personal Information Act

1. Introduction

1.1. Data protection and privacy through lawful, legitimate and responsible processing and use of personal data is a fundamental human right under the Constitution. The EOH Data Privacy Policy (this Policy) outlines the core principals which EOH endeavours to pursue in relation to the processing of personal data. The Principals set out in this Policy ensure that personal data is processed in line with regulatory requirements, industry-wide best practices and our code of conduct. The Protection of Personal Information Act (POPI Act or POPIA) and the General Data Protection Regulation (GDPR) are the primary pieces of legislation that governs how EOH collects and processes personal data.

2. Purpose

The purpose of this EOH Policy is to set out the basic principles relating to the processing of personal information. This Policy sets out how EOH process the personal data of its staff, trading partners, suppliers and other third parties.

3. Scope

3.1. This policy applies to EOH, its subsidiaries, affiliates and business employees (i.e. employees, directors, senior managers, executives, temporary staff members, agents, consultants, seconded, home-based, casual and agency staff, volunteers and interns), EOH service providers and EOH business associates and partners.

3.2. This policy is intended to assist the directors, officers, employees and appointed agents of EOH in assessing the legal position applicable to a particular decision, behaviour, conduct, act or omission.

4. Consequences of non-compliance

4.1. Wilful and deliberate non-compliance with this policy can expose EOH to significant regulatory sanctions, fines, criminal and/or civil liability. The reputational damage arising from such non-compliance will negatively affect EOH's ability to attract and maintain clients.

4.2. Employees who fail to comply with this policy may be subject to disciplinary action including dismissal and personal liability such as fines and/ or imprisonment under the relevant laws.

5. Governance and Implementation

5.1. This policy must be approved by the EOH Board of Directors.

5.2. This policy must be reviewed every two years or when a significant event occurs, taking into account any changes to regulatory requirements and business operations.

5.3. The Executives and Management of EOH are responsible for the successful implementation of the provisions of this policy.

6. Roles and responsibilities

6.1. Assigning roles and responsibilities are necessary to give effect to the requirements of this policy

6.1.1. Policy Owner

- The EOH Policy Owner is ultimately accountable for ensuring that EOH and its employees comply with the requirements set out in this process.

6.1.2. Policy Custodian

- The Policy Custodian is responsible for overseeing all dispensations, waivers and breaches to this process.
- The Policy Custodian is responsible for facilitating the review(s) as set out in the policies or standards.

6.1.3. Board of Directors and the Executive Committee

- The EOH Board of Directors and the Executive Committee are ultimately accountable for ensuring that EOH and its employees comply with the requirements set out in this policy; and
- In addition, the board must ensure that EOH complies with all applicable laws, regulations and supervisory requirements.

6.1.4. Business/Function Head

The business or function head is responsible for the following:

- Ensuring this policy is effectively implemented within their business.
- The Business Head may delegate their responsibility (but not accountability) for implementation of this policy to an appropriate executive within the business.

6.1.5. Employees

- All employees within EOH are responsible for complying with this policy.

7. Policy Principles

7.1. Processing of Data

EOH's core principles are based on the provisions of POPI and GDPR must ensure that all personal data is:

7.1.1. processed lawfully, fairly and in a transparent manner;

7.1.2. collected only for specified, clear and legitimate purposes;

7.1.3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed;

7.1.4. accurate and kept up to date where applicable;

7.1.5. not kept in a format which allows identification of a data subject for longer than is necessary for the purposes for which the data is processed;

7.1.6. processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Additionally, EOH must ensure that:

7.1.7. Personal information is not transferred to another country without appropriate safeguards being in place; and

7.1.8. EOH allows people to exercise their rights in relation to their personal data. EOH is responsible for, and must be able to demonstrate compliance with all of the above principles.

7.2. Lawfulness, Fairness and Transparency

When collecting and processing personal information for any specific purpose, EOH must always have a lawful basis for doing so. Processing personal information is lawful when at least one of the following circumstances is present:

7.2.1. the data subject has given their consent for one or more specific purposes;

7.2.2. the processing is necessary for the performance of a contract to which the data subject is a party;

7.2.3. to comply with EOH legal obligations;

7.2.4. to protect the vital interests of the data subject or another person; or

7.2.5. to pursue EOH's legitimate interests where those interests are not outweighed by the interests and rights of the person.

EOH must document the above lawful reasons relied upon when processing personal information for each specific purpose.

7.3. Consent as a lawful basis for processing

Consent may not always be the only basis for being able to process data. This will depend on the specified circumstance or scenario. A persons consent must be

7.3.1. specific;

7.3.2. informed (explained in plain and accessible language);

7.3.3. unambiguous;

7.3.4. separate and unbundled from any other terms and conditions provided to the data subject;

7.3.5. freely and genuinely given.

7.4. Openness

7.4.1. A person must be able to withdraw their consent without reservation. Once consent has been given, it will need to be updated where EOH wishes to process the personal data for a new purpose that is not compatible with the original purpose for which they were collected.

7.4.2. Chapter 6 of POPIA and Chapter 3 Section 1 of GDPR requires EOH to ensure that any information provided by EOH to people about how their personal data will be processed is concise, easily accessible, easy to understand and written in plain language. (Privacy Notice)

7.4.3. EOH must demonstrate transparency by providing people with the appropriate Privacy Notices before it collects and processes their personal information and at the appropriate times throughout the processing of their personal information.

7.4.4. Where EOH obtains any personal information about a person from a third party (for example, CVs from recruitment or background criminal checks in relation to employee on-boarding) it must check that it was collected by the third party in accordance with this policy's requirements that the sharing of such personal information with EOH was clearly explained to the person.

8. Data Minimisation

8.1. The personal information that the EOH collects and processes must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

8.2. Personal information must only be processed when necessary for the performance of duties and tasks and not for any other purposes.

8.3. Accessing of personal information where there is no authorisation to do so, or where there is no reason to access, may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

8.4. When collecting personal information, as required for the performance of duties and tasks, there should not be a request that a person provide more personal information than is strictly necessary for the intended purposes.

8.5. Where personal information is no longer needed for the specific purposes for which it was collected, such information must be deleted, destroyed and/ or anonymised.

9. Accuracy

9.1. Personal information that EOH collects and processes must be:

9.1.1. accurate and, where required and kept up-to-date; and

9.1.2. corrected and/or deleted, without delay, where an error has been discovered.

9.2. Where appropriate, any inaccurate or expired records should be deleted or destroyed.

10. Storage Limitation

10.1. The personal information that EOH collects and processes must not be kept in a form that identifies a person for longer than what is necessary in relation to the purposes for which it was collected (this is subject to compliance with any legal, accounting or reporting requirements).

10.2. There must be a regular review of any personal information which has been processed in the performance of duties to assess whether the purposes for which the information was collected has expired.

10.3. Where appropriate, reasonable steps must be taken to delete or destroy any personal data that EOH no longer requires in accordance with EOH's Record Management Policies.

10.4. All privacy notices and fair processing notices must inform data subjects of the period for which their personal data will be stored or how such period will be determined.

11. Security of Personal Information

11.1. The personal information that EOH collects and processes must be secured by appropriate technical and organisational measures against accidental loss, destruction or damage, and against unauthorised or unlawful processing.

11.2. EOH must develop, implement and maintain appropriate technical and organisational measures for the processing of personal information taking into account the:

11.2.1. nature, scope, context and purposes for such processing; and

11.2.2. the volume of personal data processed, likelihood and severity of the risks of such processing for the rights of persons.

11.3. EOH must regularly evaluate and test the effectiveness of such measures to ensure that they are adequate and effective. There is a responsibility for ensuring the security of personal information processed throughout the performance of duties.

11.4. All procedures that EOH have put in place to maintain the security of personal information from collection to destruction must be observed and adhered to.

11.5. Confidentiality, integrity and availability of personal information must be maintained at all times:

11.5.1. Confidentiality means that only people who need to know and are authorised to process any personal information can access it;

11.5.2. Integrity means that personal information must be accurate and suitable for the intended purposes;

11.5.3. Availability means that those who need to access the personal information for authorised purposes are able to do so.

11.6. Sharing personal information with third parties is prohibited unless:

11.6.1. EOH has agreed to this in advance; and

11.6.2. there has been an issuance to the respective person, of a privacy notice, beforehand and where such third party is processing the personal information on EOH's behalf.

12. Persons' Rights

12.1. Chapter 3(5) of POPIA and Chapter 3 of GDPR provides people with a number of rights in relation to their information. These rights include:

12.1.1. the right to withdraw consent unconditionally;

12.1.2. the right to be informed about how EOH collects and processes personal information;

12.1.3. the right to receive a copy of the personal information that EOH holds;

12.1.4. the right to have inaccurate personal data corrected or incomplete information completed;

12.1.5. the right to ask EOH to delete or destroy personal data if the personal data is no longer necessary in relation to the purposes for which it was collected, consent has been withdrawn (where applicable), a person has objected to the processing, the processing was unlawful, the personal information has to be deleted to comply with a legal obligation and/or the personal information was collected from a person under the age of 13 and they have reached the age of 13;

12.1.6. the right to restrict processing if there is a reasonable belief that the personal data is inaccurate;

12.1.7. the right to receive or ask EOH to transfer personal information to a third party;

12.1.8. The right to be notified of a personal data breach; and

12.1.9. The right to make a complaint to the CRO or another appropriate supervisory authority.

13. Data Protection

13.1. A Data Protection Impact Assessment (DPIA), also known as a Privacy Impact Assessment, is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data. DPIAs are required for processing personal information likely to result in high risk to the individuals and where new technologies are involved. In practice, EOH requires a DPIA for any projects involving the use of personal data, including new systems, solutions and some research studies. A DPIA must:

13.1.1. describe the nature, scope, context and purposes of the processing;

13.1.2. assess necessity, proportionality and compliance measures;

13.1.3. identify and assess risks to individuals; and

13.1.4. identify any additional measures to mitigate those risks.

14. Record Retention

All records pertaining to this policy should be retained in accordance with EOH's internal record retention policy.