DATA PROTECTION IMPACT ASSESSMENT POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for data protection impact assessment by the GDPR.

2 SCOPE

This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by ZEN KNOTWEED LTD and to all employees, including part-time, temporary, or contract employees, that handle personal data.

3 POLICY STATEMENT

Data Protection Impact Assessments (DPIA) are used to identify and mitigate against any data protection related risks arising from a new project, service, product, or process, which may affect the organization (Data Controller) or the individuals (Data Subjects).

When is DPIA necessary

3.1 DPIA is necessary:

- Before the implementation of new technologies or processes, or before the modification of existing technologies or processes;
- Data processing is likely to result in a high risk to the rights and freedoms of individuals.

3.2 Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals;
- Large scale processing of special categories of data or personal data relation to criminal convictions or offences;
- Large scale, systematic monitoring of public areas (CCTV).

Should the Regulator be consulted on completion of the DPIA

3.3 If, during the DPIA process, the Data Controller has identified and taken measures to mitigate any risks to personal data, it is not necessary to consult with the Regulator before proceeding with the changes.

3.4 If the DPIA suggests that any identified risks cannot be managed and the residual risk remains high, you must consult with the Regulator before moving forward with the project.

3.5 Regardless of whether or not consultation with the Regulator is required, your obligations of retaining a record of the DPIA and updating the DPIA in due course remain.

3.6 Even if consultation is not required, the DPIA may be reviewed by the Regulator at a later date in the event of an audit or investigation arising from your use of personal data.

4 PROCEDURE

Steps for conducting DPIA

4.1 **Describe data flows.** Identify how personal information will be collected, stored, used and deleted as part of the new (or modified) system or process. Identify what kinds of data will be used as part of the new (or modified) system or process and who will have access to the data. *Populate Section 1 of the Data Protection Impact Assessment (DPIA) Form.*

4.2 **Identify data protection and related risks.** Identify all risks to Data Subjects or to the organization (Data Controller) that are related to personal data protection. For each risk assign a risk category (High/Medium/Low) and *populate the appropriate columns in Section 2 of the Data Protection Impact Assessment (DPIA) Form.*

4.3 **Assign risk mitigation measures.** For each risk assign risk mitigation measures. Focus on mitigating measures for risks with High and Medium impact category. *Populate the last column in Section 2 of the Data Protection Impact Assessment (DPIA) Form.*

4.4 **Further actions.** Consider if the Regulator should be consulted for the DPIA. Plan regular DPIA reviews and updates.

5 RESPONSIBILITIES

Compliance, monitoring and review

5.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing data protection impact assessment activities at ZEN KNOTWEED LTD rests with the Data Protection Officer.

5.2 All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant ZEN KNOTWEED LTD policies and procedures.

Records management

5.3 Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised ZEN KNOTWEED LTD recordkeeping system.

5.4 All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

6 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

7 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Data Protection Act 2018
- ZEN KNOTWEED LTD Data Protection Policy

8 FEEDBACK AND SUGGESTIONS

8.1 ZEN KNOTWEED LTD employees may provide feedback and suggestions about this document by emailing suggestiona@zenknotweed.com.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	CEO
Data Protection Officer	Anthony Chamberlain
Next Review Date	10/06/2020

Approval and Amendment History	Details
Original Approval Authority and Date	CEO 10/06/2019
Amendment Authority and Date	Anthony Chamberlain 10/06/2020

11 APPENDIX

Please attach the Data Protection Impact Assessment (DPIA) Form.