Data Protection and GDPR Policy

Purpose

This policy sets out our requirements so that riskHive can protect individuals' fundamental rights and freedoms, particularly their right to protection of their personal data.

Article 5 of the Data Protection Act 2018 requires that personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency').

(b) 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 shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 Data Protection Act in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

This policy applies to all personal data process by riskHive Software Solutions Ltd and riskHive Technical Services Ltd.

Responsibilities

The **Managing Director** is responsible for:

- Reviewing, endorsing, and achieving this policy's aims.
- Ensuring ongoing compliance to this policy and is the responsible person for Data Protection.

riskHive employees are responsible for:

- Carrying out their work in line with this policy and associated procedures.
- Identifying any breaches of this policy and reporting them to the appointed Data Protection Officer (Sandu Hellings).

Requirements

To comply with the requirements of the Data Protection Act 2018, riskHive shall:

General Provisions

- Register with the Information Commissioner's Office (ICO) as an organisation that processes personal data.

Lawful, fair and transparent processing

- Maintain a Register of Systems, which will be reviewed annually.
- Allow individuals have access to their personal data and any such requests made will be dealt with in a timely manner.

Lawful purposes

- Process data on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task, or legitimate interests, with the appropriate lawful basis noted in the Register of Systems.
- Keep evidence of opt-in consent with the personal data, where consent is relied upon as a lawful basis for processing said data.
- Allow individuals to revoke their consent. This process will be clearly available with systems in place in place to ensure such revocation is reflected accurately in our records.

Data minimisation

- Ensure that personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

- Take reasonable steps to ensure personal data is accurate.
- Take the necessary steps to ensure, (where necessary for the lawful basis on which data is processed) that personal data is kept up to date.

Archiving / removal

- Ensure that personal data is kept for no longer than necessary, in accordance with our **Information Management Procedure.** This includes what data should/must be retained, for how long and why.

Security

- Ensure that personal data is stored securely using software that is kept-up to date with adequate back-up.
- Ensure that access to personal data is limited to personnel who need access with appropriate security in place to avoid unauthorised sharing of information.
- Delete personal data safely, such that the data is irrecoverable.
- Invoke our Business Continuity Arrangements should a catastrophic event occur.

Breach

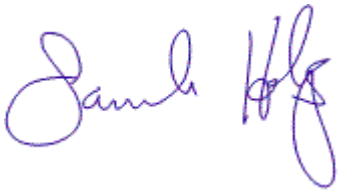
- Promptly assess the risk to the people's rights and freedoms should a breach of security occur which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- If appropriate, report this breach to the ICO.

Measure of success

We measure our success of the implementation of this policy by:

- Being able to demonstrate to our customers that we have not experienced any Data Protection Act Breaches.

Signature and date



24.02.2023

Sandu Hellings – Managing Director / Data Protection Officer