Fjelltopp policy on Security and Data Management

Fjelltopp Ltd will gather and use certain information about individuals and will work with clients to manage their potentially confidential data. The internal data can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. Client data will include everything from public data sets to patient confidential data. This policy describes how this data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

Why this policy exists

This data protection policy ensures Fjelltop Ltd:

- Complies with all data protection laws and follows good practice for data management.
- Protects the rights of staff, customers and partners.
- Protects clients and their data
- Is open about how it stores and processes data
- Protects itself from the risks of a data breach

General Considerations

1. This policy applies to all data processed by Fjelltopp Ltd.
2. The Fjelltopp CTO shall take responsibility for Fjelltopp's ongoing compliance with this policy.
3. This policy shall be reviewed at least annually.
4. Fjelltopp shall register with the Information Commissioner's Office as an organisation that processes personal data.

Data protection law

Fjelltopp LTD is committed to processing data in accordance with its responsibilities under the General Data Protection Regulation (GDPR). For data stored or processed on behalf of clients, the data protection act or similar law for the country of the client shall be followed in addition to the principles in the GDPR.

Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. 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;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. 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;
5. 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 1998 purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. 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."

Policy scope

This policy applies to:

- All directors and members of Fjelltopp Ltd
- All staff and volunteers of Fjelltopp Ltd
- All consultants, contractors, suppliers and other people working on behalf of Fjelltopp Ltd.
- All data that the company holds.

Data protection risks

This policy helps to protect Fjelltopp from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, the information being given out inappropriately.
- **Failing to offer a choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Sharing of Data

Fjelltopp processes data with a large range of confidentiality from public data sets to patient confidential data. Before any data is shared publicly or with any third-party, it is essential with permission from the data owner. Any data that has not already been shared publicly or where specific consent for sharing shall be considered confidential and shall not be shared with any third-party.

Sharing of Computer code and Open Source

Fjelltopp has a commitment to open source code. If there are no reasons for keeping source code confidential, the source code should be made open source with appropriate open source licences. Code fulfilling any of the following criteria shall not be made open source

- The code is developed for a client without agreement from the client that the code can be shared
- The code contains any information that can be considered confidential
- The code contains Fjelltopp specific deployment or infrastructure information

Data Security

1. Fjelltopp shall ensure that personal data is stored securely using modern software that is kept up-to-date.
2. For highly confidential data encryption at rest should always be the aim
3. Access to data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
4. A record of who has access to which data shall be kept.
5. When personal data is deleted this should be done safely such that the data is irrecoverable.
6. Appropriate backup and disaster recovery solutions shall be in place.
7. All passwords used to access data needs to be strong and follow best practise guidelines. This includes not reusing passwords.
8. If confidential data is stored on personal devices they should employ encryption or other counter-measures to avoid data leaks if the personal device is stolen.

Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Fjelltopp Ltd shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).