ChangeWave Information Handling and Privacy Policy

Version 1.2

20 August 2019

1 Introduction

In order to provide services to clients, ChangeWave collects, collates and analyses business and personal data from its clients and people involved in the client's business, business partners, associates and business contacts. Data Subjects are the people or companies about whom we store data. This information needs to be treated carefully to ensure appropriate confidentiality is maintained.

This document describes the information security operating principles to be adopted by ChangeWave and people working for ChangeWave. These principles are aimed at providing appropriate data security for a small organisation and compliance with EE directive on General Data Protection Regulations (GDPR) that comes into force on 25 May 2018.

ChangeWave will not share (or sell) any client or individual's information without their permission.

2 Permission to collect data

In the normal course of business, routine contacts with clients and people involved in the client's business, suppliers, business partners and others will be collected to facilitate ongoing communication. This includes business contact data such as Name, Role, Telephone numbers and email addresses. ChangeWave will not seek formal permission to store this business contact data but recognises its sensitivity as described below.

During formal discussions and contracting with clients, potential clients, business partners and associates ChangeWave will explicitly recognise and advise that data, both personal and business related, may be collected and processed in order that ChangeWave can provide services in a professional manner.

3 Information types

Four classes of information are envisaged:

1. **Business contact data** - general contact data as described above for business communication
2. **Personal contact data –** personal contact details that allow an individual to be identified outside of work e.g. personal telephone number or home address
3. **Sensitive Personal data**. – in provision of services, sensitive personal data may become known to ChangeWave personnel. As defined under the Data Protection Act 1998 this includes:
    a. racial or ethnic origin of the data subject,
    b. political opinions,
    c. religious beliefs or other beliefs of a similar nature,
    d. membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
    e. physical or mental health or condition,
    f. sexual life,

g. Commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed.
h. any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.]

Ways in which data are collected include but are not limited to: meeting notes, coaching logs, psychometric test results, personal objectives, answers to questionnaires, 360 degree / other feedback and performance reviews, interviews with staff prior to team meetings and workshops and team meeting and workshop slides and outputs.

4. **Sensitive Company data**. This is limited to information that is not in the public domain or easily deduced from information within the public domain. This includes strategic intent, information on organisation structure, commercial position, potential staff moves, workshop inputs and outputs, intellectual property etc.

4. Information treatment

The above information classes will be treated separately

Business contact data and personal contact data

This information is primarily contained in Contacts databases, emails and appointment calendars. ChangeWave will use externally hosted email, contacts and calendar services. A professional, established application with active security oversight and updating will be utilised. (Currently Microsoft Exchange is used through the Office 365 subscription and is therefore fully updated and includes the latest security controls). All information exchanged with the service provider will be encrypted. The service provider is expected to comply with all relevant EE directives and standards in providing security of the data with respect to its services.

Where there is a reasonable expectation that introducing one person to another will be beneficial, ChangeWave will request permission to share contact email and other contact details with the other party.

Contact data is stored by ChangeWave personnel as long as it is considered useful for normal business needs.

Sensitive Personal and Company Data

Electronic versions of data will be stored on the internal ChangeWave network. Any paper copies or hand-written notes will be stored securely at ChangeWave's office.

Such data will be shared only with Data Subjects and others whom they have specified.

ChangeWave will always request a client's permission before using their feedback in any testimonial or case study.

If we need to take electronic data outside of the ChangeWave office this data will be carried will be carried in an encrypted or password protected way.

Most of our clients require us to have Professional Indemnity Insurance and for this insurance companies require data to be held for 7 years. This is our default storage period. Seven years after a programme or piece of work is completed, all paper versions will be shredded and electronic copies deleted.

5 Data Subjects Rights

There are a number of statutory rights and how we handle these is covered below:

1. Subject Rights Access – an individual can seek to obtain confirmation as to whether or not personal data concerning them is being processed by ChangeWave, where and for what purpose. These are specified in our terms of business and clients will have agreed to them before any engagement starts. Subjects also have the right to be provided with a copy of that personal data free of charge.
2. The Right to be Forgotten – All data including the classifications above are normally stored for seven years to meet the general requirements for professional indemnity insurance that most clients require. Should an individual request that data is destroyed, then all sensitive personal data will be deleted as soon as possible in primary data stores and all back-up stores. Note that ChangeWave will not delete data that shows that a commercial arrangement has been in place. This includes meeting dates, invoices etc. and data that is required for legal and tax purposes. There are a number of exceptions to the automatic deletion of data upon request:
    a. If the provision of services is still ongoing, then suitable service termination arrangements are to be complete first.
    b. If, in the opinion of ChangeWave, such data may be relevant in potential criminal investigations then it will be retained.
    c. If such personal data or sensitive personal data is required to be held for professional indemnity reasons (see 4 above), then individuals and organisations must waive any future rights to action in this regard before data is deleted.
    d. If there is any dispute or ongoing action with the individual or organisation any information deemed by ChangeWave to be materially relevant will be held until such dispute is resolved.
3. The Right to Rectification – this means that an individual can seek to have personal data held on them corrected without undue delay where the data concerning them is inaccurate.
4. The Right to Restriction – this means that an individual can seek to restrict processing of the personal data held on them, subject to certain conditions. In ChangeWave this is likely to be associated with an end to the services provided and the conditions under “Right to be forgotten” would apply.
5. The Right to Object to Processing – An individual can object to processing personal data held on them.

6. The Right to Portability – this means that an individual can receive the personal data concerning them in a "structured, commonly used and machine-readable format".
7. The Right to Lodge a Complaint with a Data Protection Regulator – this means that an individual can make a complaint before a regulator about data protection issues concerning them.

6 Security Breaches

If any ChangeWave employee, associate or supplier becomes aware of leakage or breach of security on sensitive information, or of systemic loss of personal data (eg mail service provider has suffered a theft of personal data), then the data controller must ensure that relevant clients or individuals are contacted as soon as possible advising of the breach, the data lost and an action plan agreed.

7 Statutory Roles

E Maguire is the Data Protection Officer and can be contacted at eddie.maguire@changewave.co.uk

8 Approvals & reviews

This document has been approved by ChangeWave Directors. It will be reviewed at least annually and when material changes are required. Next review due before 20 August 2020