General Data Protection Regulations Policy

Coventry & Warwickshire Chamber of Commerce Training

Training | Skills | Growth

1. Introduction

This Policy sets out the obligations of Coventry & Warwickshire Chamber of Commerce Training regarding the rights of data protection and processing in respect of personal data under DPA 2018 and UK General Data Protection Regulation (UK GDPR).

The UK GDPR defines personal data as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data relating to data subjects. The procedures and principles set out must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

Coventry & Warwickshire Chamber of Commerce Training is committed to the law and places high importance on the correct, lawful and fair handling of all personal data. The Chamber respects legal rights, privacy and the trust of all individuals in which data is kept.

2. Failure of Compliance

Employees should be aware that if any data (as specified throughout this policy) is used, processed or handled in a way that may be deemed as deliberate or inadvertent misuse, could be in breach of these guidelines. This may lead to disciplinary action under Coventry & Warwickshire Chamber of Commerce Training's disciplinary procedure. Serious breaches of these guidelines may constitute gross misconduct and may lead to action under the disciplinary procedure up to and including dismissal.

How Employees Process and Handle Personal Data:

3. The Data Protection Principles

This Policy aims to ensure compliance with the UK GDPR. The UK GDPR sets out the following principles with which any employee handling personal data must comply. All personal data must be:

3.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject;

3.2 Collected for specified, explicit, and legal or legitimate purposes and not further processed in a manner that is incompatible with those purposes;

3.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;

3.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, is erased, or rectified without delay (when necessary and appropriate);

3.5 Kept in a safe and secure environment which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;

3.6 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 put in place by Managers.

Reasons for Employees Processing Personal Data:

4. Lawful, Fair, and Transparent Data Processing

4.1 The UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The UK GDPR states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;

4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;

4.1.5 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party;

Special Category Data (Sensitive Personal Data):

4.2 If the personal data in question is special category data (also known as sensitive personal data, for example, data concerning the data subject's race, ethnicity, politics, religion, genetics, health, sex life, or sexual orientation, at least one of the following conditions must be met:

4.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes;

4.2.2 The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law;

4.2.3 The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

4.2.4 The processing relates to personal data which is clearly made public by the data subject;

4.2.5 The processing is necessary for the conduct of legal claims;

4.2.6 The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment;

Where employees are processing Special Category Data, it must be for one of the purposes as outlined above.

5. Personal Data collected, Held and Processed

5.1 The Company collects and processes personal data on a wide scale in compliance with this Policy. Line managers will be responsible for periodically reviewing the way in which data is processed and held in accordance with UK GDPR regulations. Employees will be informed specifically of the data rules within their individual teams which will be communicated by their Manager. If employees fail to adhere to these rules, this may result in Disciplinary action.

Personal Data held on Employees:

6. Employee Personal Data

The Company holds personal data that is directly relevant to its employees. That personal data shall be collected, held, and processed in accordance with employee data subjects' rights and the Company's obligations under the UK GDPR and with this Policy. The Company will collect, hold and process personal data specified below in relation to its employees. This data includes but not limited to:

6.1 Identification information relating to employees:

6.1.1 Name;

6.1.2 Contact Details, including but not limited to; Address, Date of Birth and National Insurance number;

6.1.3 Emergency Contact and Next of kin information.

6.2 Equal opportunities monitoring information:

6.2.1 Age;

6.2.2 Gender;

6.2.3 Ethnicity;

6.2.4 Nationality;

6.2.5 Religion;

6.2.6 Marital Status.

6.3 Health records:

6.3.1 Details of sick leave;

6.3.2 Medical conditions;

6.3.3 Disabilities;

6.3.4 Prescribed medication.

6.4 Employment records:

6.4.1 Interview notes;

6.4.2 CVs, application forms, covering letters, and similar documents;

6.4.3 Assessments, performance reviews, and similar documents;

6.4.4 Details of remuneration including salaries, pay increases, bonuses, commission, overtime, benefits, and expenses;

6.4.5 Employee monitoring information;

6.4.6 Records of disciplinary matters including reports and warnings, both formal and informal;

6.4.7 Details of grievances including documentary evidence, notes from meetings, procedures followed, and outcomes.

7. Health Records

7.1 The Company holds health records on all employee data subjects which are used to assess the health, wellbeing, and welfare of employees and to highlight any issues which may require further investigation. In particular, the Company places a high priority on maintaining health and safety in the workplace, on promoting equal opportunities, and on preventing discrimination on the grounds of disability or other medical conditions. In most cases, health data on employees falls within the UK GDPR's definition of special category data. Any and all data relating to employee data subjects' health, therefore, will be collected, held, and processed strictly in accordance with the conditions for processing special category personal data.

7.2 Health records shall be accessible and used only by the HR Department, Executive Team or when applicable, the Employee's Manager and shall not be revealed to other employees, agents, contractors, or other parties working on behalf of Coventry & Warwickshire Chamber of Commerce Training without the express consent of the employee data subject(s) to whom such data relates. Except in exceptional circumstances where the wellbeing of the employee(s) (data subject) to whom the data relates is at stake.

Health records will only be collected, held, and processed to the extent required to ensure that employees are able to perform their work correctly, legally, safely, and without unlawful or unfair impediments or discrimination.

8. Benefits

8.1 In cases where employee data subjects are enrolled in benefit schemes which are provided by the Company, it may be necessary from time to time for third party organisations to collect personal data from relevant employee data subjects.

8.2 The Company shall not use any such personal data except as and when necessary for the purpose of the administration of the relevant benefits schemes.

8.3 The following schemes are available to employees. Please note that not all schemes may be applicable to all staff:

8.3.1 SimplyHealth – Healthcare Cash Plan Scheme -(Broker HealthMatters)

8.3.2 Scottish Widows – Pension Scheme (Broker – Wrensterling)

8.3.3 BUPA – Private Medical Insurance (Broker – Jelf Group)

8.3.4 Metlife – Life Insurance Policy (Broker – Wrensterling)

8.3.5 Any other relevant Employee Benefit Schemes

8.3.6 For further information on personal details provided to the organisations specified above, please contact the Executive Director.

9. Employee Monitoring

9.1 The Company may from time to time monitor the activities of employee data subjects. Such monitoring may include, but will not necessarily be limited to, internet, phone and email monitoring.

9.2 Monitoring should not (unless exceptional circumstances justify it) interfere with an employee's normal duties.

9.3 Monitoring will only take place if the Company considers that it is necessary to achieve the benefit it is intended to achieve. Personal data collected during any such monitoring will only be collected, held, and processed for reasons directly related to (and necessary for) achieving the intended result and, at all times, in accordance with employee data subjects' rights and the Company's obligations under the UK GDPR.

9.4 The Company shall ensure that there is no unnecessary intrusion upon employee data subjects' personal communications or activities, and under no circumstances will monitoring take place outside of an employee data subject's normal place of work or work hours, unless the employee data subject in question is using Company equipment or other facilities including, but not limited to, Company email, Company Phone or the Company network.

10. Accuracy of Data and Keeping Data Up-to-Date

10.1 The Company shall ensure that all personal data collected, processed, and held is kept accurate and up-to-date.

10.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

11. Data Retention

11.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

11.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

Line Managers will implement reasonable practices to ensure that all data is monitored regularly to reduce the risk of unnecessary data. Managers will ensure that there is a clear process in place in regards to the removal of personal data from the company's database. It is the Employee's responsibility to carry out these practices accordingly.

12. Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

Steps such as encryption for e-mails are in place to reduce the risks of security breaches as well as incorrect processing and handling of data in compliance with UK GDPR. Paper based files should be stored away securely at all times when appropriate. Further security measures can be implemented at any time as and when the company deems necessary and all employees are expected to follow new and existing procedures. Failure to do so may result in Disciplinary action.

13. Accountability and Record-Keeping

All Employees employed by Coventry & Warwickshire Chamber of Commerce Training understand that they are responsible for collecting, handling and processing data in line with the UK GDPR regulations and all other applicable data protection legislation. The Executive Team and the HR Department are responsible for implementing this Policy. Line Managers and employees are responsible for the monitoring of compliance throughout the Organisation. The Company shall keep written internal records of data collection, holding, and processing.

14. Data Security - Storage

Coventry & Warwickshire Chamber of Commerce Training shall ensure that all personal data kept is stored securely with limited accessibility. The following measures are taken to ensure data is kept secure:

14.1 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar.

Personal data will generally be stored on our CRM systems such as PICS, RUBI and Evolutive. It is both the Line Managers and the Employees responsibility to ensure all data collected is monitored regularly and appropriately.

In some circumstances, it may be required for Employees to keep client paper based personnel files, particularly for Advisors. Line Managers will clearly specify the companies guidelines in regards to handling this information including; the length of time an employee can hold personal data and the companies policy on how personal data should be stored. Both Line Managers and employees will have a detailed structure in place defining the steps of handling, recording and processing personal data.

15. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Line Managers will be responsible for implementing a clear process for any personal data in circumstances where this is necessary.

16. Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

16.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested.

16.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the relevant Line Manager;

16.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

16.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

16.5 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Employee to ensure that the appropriate consent is obtained and that no data subjects have opted out.

17. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

17.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the UK GDPR and under this Policy;

17.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

17.3 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

17.4 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed by Line Managers and Team Leaders;

17.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the UK GDPR and this Policy by contract;

17.6 Where any employee, agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy, that party and/or individual shall take full responsibility against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

18. Data Breach Notification

18.1 All personal data breaches must be reported immediately to the Executive Director.

18.2 Refer to the Data Protection Policy for data breach procedure.

19. Implementation of Policy

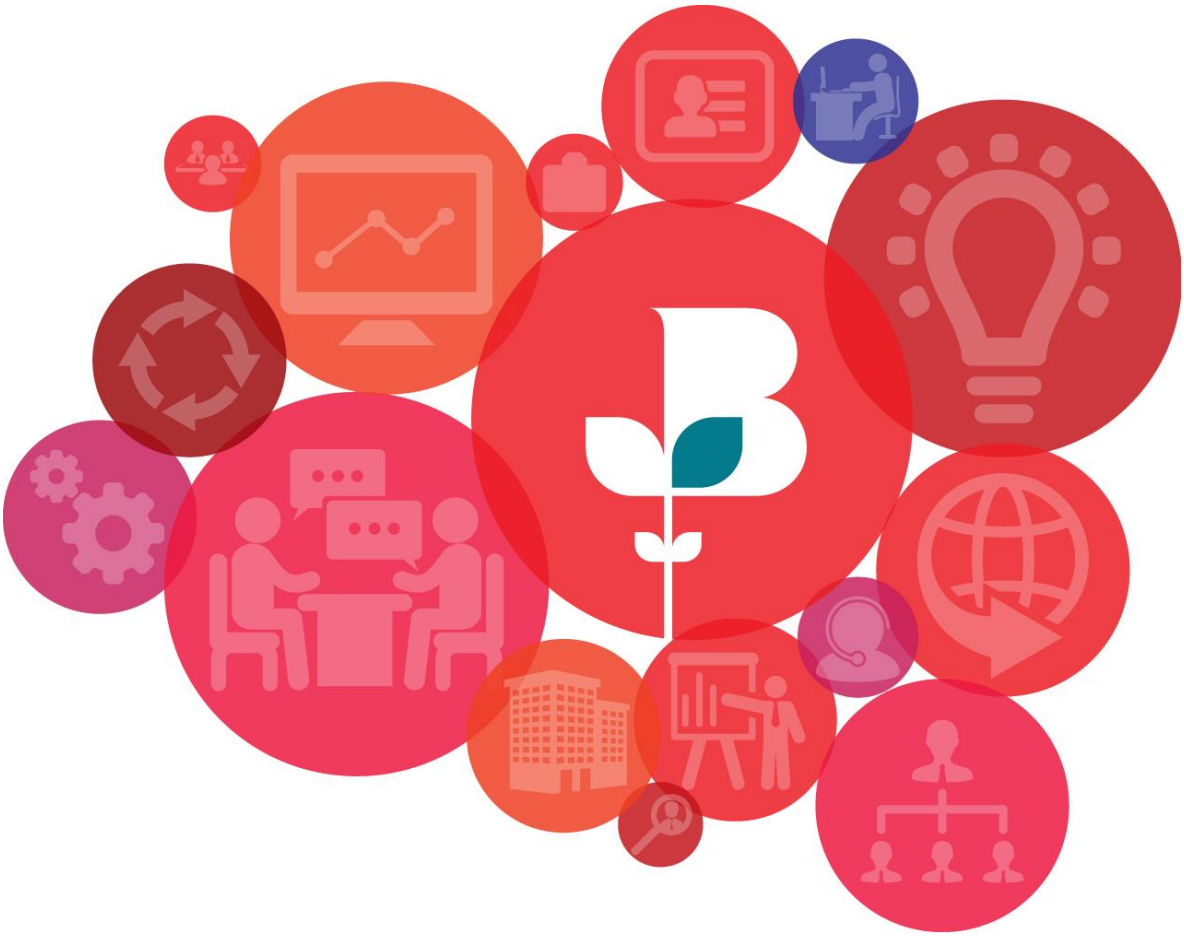
19.1 This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

19.2 This Policy operates in conjunction with the Company's Privacy Policy and Data Protection Policy.

19.3 This policy will be reviewed annually.

20. Executive Approval

This Policy has been approved and authorised by the organisation's Executive Management team.



moving forward Together