



Data Protection Policy

May 2018

1. Introduction

This Policy sets out the obligations of Endorse HR (“the Company”) regarding data protection and the rights of clients and stakeholders (“data subjects”) in respect of their personal data under the General Data Protection Regulation (“the Regulation”).

The Regulation 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 out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

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

- a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- 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;
- c) adequate, relevant and limited to what is necessary in relation to the purposes

for which it is processed;

- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
- 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 is 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 Regulation in order to safeguard the rights and freedoms of the data subject;
- 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.

3. Lawful, Fair, and Transparent Data Processing

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

- a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- b) 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;
- c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- d) processing is necessary to protect the vital interests of the data subject or of another natural person;
- e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4. Processed for Specified, Explicit and Legitimate Purposes

4.1 The Company collects and processes the personal data set out in Part 19 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from clients or third parties (for example, an occupational health report received from the client or an

occupational health provider).

4.2 The Company only processes personal data for the specific purposes set out in Part 19 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

5. **Adequate, Relevant and Limited Data Processing**

The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. **Accuracy of Data and Keeping Data Up To Date**

The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at annual intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. **Timely Processing**

The Company shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

8. **Secure Processing**

The Company shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 20 and 21 of this Policy.

9. **Accountability**

9.1 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- a) The name and details of the Company and any applicable third party data controllers;
- b) The purposes for which the Company processes personal data;
- c) Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates as detailed in Schedule 1;
- d) Details (and categories) of any third parties that will receive personal data from the Company;
- e) Details of how long personal data will be retained by the Company as detailed

in Schedule 1; and

- f) Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data as detailed in Schedule 2.

10. **Privacy Impact Assessments**

The Company shall carry out Privacy Impact Assessments when and as required under the Regulation and shall address the following areas of importance:

- 10.1 The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;
- 10.2 Details of the legitimate interests being pursued by the Company;
- 10.3 An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- 10.4 An assessment of the risks posed to individual data subjects; and
- 10.5 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

11. **The Rights of Data Subjects**

The Regulation sets out the following rights applicable to data subjects:

- a) The right to be informed;
- b) The right of access;
- c) The right to rectification;
- d) The right to erasure (also known as the 'right to be forgotten');
- e) The right to restrict processing;
- f) The right to data portability;
- g) The right to object;
- h) Rights with respect to automated decision-making and profiling.

12. **Keeping Data Subjects Informed**

12.1 The Company shall ensure that the following information is provided to every data subject when personal data is collected:

- a) Details of the Company including, but not limited to, the identity of Michael Green, Director and Owner of Endorse HR Limited;
- b) The purpose(s) for which the personal data is being collected and will be

processed (as detailed in Part 19 of this Policy) and the legal basis justifying that collection and processing;

- c) Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
- d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- e) Where the personal data is to be transferred to one or more third parties, details of those parties;
- f) Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined) as described in Schedule 1;
- g) Details of the data subject's rights under the Regulation;
- h) Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;
- i) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);
- j) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;
- k) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

12.2 The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:

12.2.1 Where the personal data is obtained from the data subject directly, at the time of collection;

12.2.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

- a) If the personal data is used to communicate with the data subject, at the time of the first communication; or
- b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or
- c) In any event, not more than one month after the time at which the Company obtains the personal data.

13. **Data Subject Access**

13.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt

(this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

- 13.2 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. **Rectification of Personal Data**

14.1 If a data subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

14.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

15. **Erasure of Personal Data**

15.1 Data subjects may request that the Company erases the personal data it holds about them in the following circumstances:

- a) It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;
- b) The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
- c) The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 17 of this Policy for further details concerning data subjects' rights to object);
- d) The personal data has been processed unlawfully;
- e) The personal data needs to be erased in order for the Company to comply with a particular legal obligation;

15.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

15.3 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. **Restriction of Personal Data Processing**

- 16.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.
- 16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. **Objections to Personal Data Processing**

- 17.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific or and statistics purposes.
- 17.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.
- 17.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith.
- 17.4 Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

18. **Profiling**

Where the Company uses personal data for profiling purposes, the following shall apply:

- a) Clear information explaining the profiling will be provided, including its significance and the likely consequences;
- b) Appropriate mathematical or statistical procedures will be used;
- c) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and
- d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 20 and 21 of this Policy for more details on data security).

19. **Personal Data**

The following personal data may be collected, held, and processed by the Company:

- a) Staff data: copies of contracts, supervision records, personal and contact details, date of birth, family and next of kin details, occupational health reports, fit for work notes, self-certification records, training records, grievance and disciplinary records.
- b) Data is collected, held and processed so that we are able to ensure that we respect the Data Controller's agreed pay and conditions, are able to contact next of kin in case of an emergency, can support staff members adequately in case of sickness and are able to performance manage effectively, DBS details;
- c) Client data: contact details, copies of contracts and agreements for specific pieces of work, emails between the organisations, documents necessary for effective completion of case work in both electronic and hard-copy format;

20. **Data Protection Measures**

The Company shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

- a) Where 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. Hardcopies should be shredded, and electronic copies should be deleted securely.
- b) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- c) Personal data will only be transmitted over a public wireless network using an encrypted and secure virtual private network [VPN].
- d) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- e) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- f) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient;
- g) 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 from Michael Green.
- h) 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;

- i) 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 Michael Green;
- j) 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;
- k) 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;
- l) Personal data stored on any mobile device must be password protected (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise.
- m) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);
- n) Office 365's secure, encrypted systems are used to store and back up all personal data electronically.
- o) All electronic copies of personal data should be stored securely using passwords and data encryption;
- p) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Company is designed to require such passwords;
- q) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.
- r) Where personal data held by the Company is used for marketing purposes, it shall ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least annually.

21. **Organisational Measures**

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

- a) 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 Regulation and under this Policy,

and shall be provided with a copy of this Policy;

- b) 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;
- c) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- d) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
- f) The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- g) 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 Regulation and this Policy by contract;
- h) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation;
- i) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

22. Data Breach Notification

- 22.1 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), Michael Green must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- 22.2 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- 22.3 Data breach notifications shall include the following information:
 - a) The categories and approximate number of data subjects concerned;
 - b) The categories and approximate number of personal data records concerned;
 - c) The name and contact details of the Company's point of contact;

- d) The likely consequences of the breach;
- e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

23. Implementation of Policy

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

This Policy has been approved and authorised by:

Name: Michael Green

Position: Director Endorse HR Ltd

Date: 15 May 2018

Due for Review by: 31 May 2020

Signature:

SCHEDULE 1

Personal Data

Type of Data	Source	Purpose	Description	Where held?	Justification	Legal statute/ business purpose	Legal reason for retention	Legal retention period	Currently proposed retention period.
Case Work Investigations Hearings Projects	Client	Case management	Case, contact and personal data	Office 365 for Business digital folder. Desk top hard drive back-up	Legitimate interest	Business			Until completion of case and any potential appeal limitation period when all data is returned to the client or destroyed
Tribunal preparation and bundles of evidence	Client	Case management	Case, contact and personal data	Ditto	Legitimate interest	Business			Until completion of case and any potential appeal limitation period when all data is returned to the client or destroyed
Employee contact information	Employee	Employee management	Contact information for employees.	Ditto	Contract	Business			6 years after employment end.
Employee bank information	Employee	Employee management	Bank account/ pay details for employees.	Ditto	Contract	Business			6 years after employment end.
Proof of right to work	Passport	Recruitment and retention.	Signed and dated copy of employment details.	Ditto	Legal requirement	Statute	Sec. 15 Assylum and Nationality Act 2006		6 years after employment end.

Application forms for unsuccessful candidates.	Candidates	Recruitment and retention.	Candidate contact information	Ditto	Legitimate interest	Advisory			6 Months
Personnel and training files	Multiple	Employee management	Training details	Ditto	Contract	Advisory	Limitation Act 1980		6 years after employment end.
Records relating to working time	Management	Employee management	Records of hours worked, time-sheets and/or overtime records.	Ditto	Legal requirement	Statute	The Working Time Regulations 1998 (SI 1998/1833)	2 years from date on which they were made.	6 years after employment end.
Redundancy details	Management and Employee	Employee management	Redundancy records	Ditto	Legitimate interest	Advisory	Limitation Act 1980		6 years from date of redundancy.
Senior executives' records.	Management and Employee	Asset management.	Contact information for senior executives	Ditto	Public interest	Advisory			Permanent.
Occupational Health records	Management and Employee	Employee management	Health assessments of employees	Ditto	Legitimate interest	Advisory			6 years after employment end.
Statutory Sick Pay records.	Management and Employee	Employee management	Sick pay records	Ditto	Legitimate interest	Advisory	Limitation Act 1980		6 years
Health and Safety Assessments	Management and Employee	Health and Safety	Health and Safety	Ditto	Legitimate interest	Advisory	Health and Safety at Work etc Act 1974	3 years from the assessment	Permanent.

SCHEDULE 2

Technical and Organisational Data Protection Measures

1. The following are the technical and organisational data protection measures referred to in Clause 4:
 - 1.1. The Data Processor shall ensure that, in respect of all Personal Data it receives from or processes on behalf of the Data Controller, it maintains security measures to a standard appropriate to:
 - 1.1.1. the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Personal Data; and
 - 1.1.2. the nature of the Personal Data.
 - 1.2. In particular, the Data Processor shall:
 - 1.2.1. have in place, and comply with a data protection policy which:
 - 1.2.1.1. defines security needs based on a risk assessment;
 - 1.2.1.2. allocates responsibility for implementing the policy to a specific individual;
 - 1.2.1.3. is provided to the Data Controller on or before the commencement of this Agreement;
 - 1.2.1.4. is disseminated to all relevant staff; and
 - 1.2.1.5. provides a mechanism for feedback and review.
 - 1.2.2. ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;
 - 1.2.3. prevent unauthorised access to the Personal Data;
 - 1.2.4. protect the Personal Data using pseudonymisation, where it is practical to do so;
 - 1.2.5. ensure that its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;
 - 1.2.6. have secure methods in place for the transfer of Personal Data whether in physical form or electronic form;
 - 1.2.7. password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure, and that passwords are not shared under any circumstances;

- 1.2.8. take reasonable steps to ensure the reliability of personnel who have access to the Personal Data;
- 1.2.9. have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including:
 - 1.2.9.1. the ability to identify which individuals have worked with specific Personal Data;
 - 1.2.9.2. having a proper procedure in place for investigating and remedying breaches of the GDPR; and
 - 1.2.9.3. notifying the Data Controller as soon as any such security breach occurs.
- 1.2.10. have a secure procedure for backing up all electronic Personal Data and storing back-ups separately from originals;
- 1.2.11. have a secure method of disposal of unwanted Personal Data including for back-ups, disks, print-outs, and redundant equipment; and
- 1.2.12. adopt such organisational, operational, and technological processes and procedures as are required to comply with the requirements of ISO/IEC 27001:2013, as appropriate to the Services provided to the Data Controller.