Company Name:	Extraman Limited
Document DP3	Data Protection Policy
Topic:	Data protection
Date:	May 2018
Version:	V2 - 18

Contents

All organisations that process *personal data* are required to comply with data protection legislation. This includes in particular the Data Protection Act 1998 (or its successor) and the EU General Data Protection Regulation (together the 'Data Protection Laws'). The Data Protection Laws give individuals (known as 'data subjects') certain rights over their *personal data* whilst imposing certain obligations on the organisations that process their data.

As a recruitment business Extraman Limited collects and processes both *personal data* and *sensitive personal data*. It is required to do so to comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data.

This policy sets out how Extraman Limited implements the Data Protection Laws. It should be read in conjunction with the Data Protection Procedure.

In this policy the following terms have the following meanings:

'*consent*' means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the *processing* of persona data relating to him or her;

'*data controller*' means an individual or organisation which, alone or jointly with others, determines the purposes and means of the *processing* of *personal data*;

'*data processor*' means an individual or organisation which processes *personal data* on behalf of the *data controller*;

'*personal data*'* means any information relating to an individual who can be identified, such as by 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.

'*personal data breach*' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *personal data*;

'*processing*' means any operation or set of operations performed on *personal data*, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'*profiling*' means any form of automated *processing* of *personal data* consisting of the use of *personal data* to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

'*pseudonymisation*' means the *processing* of *personal data* in such a manner that the *personal data* can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the *personal data* are not attributed to an identified or identifiable individual;

'*sensitive personal data*'* means *personal data* revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the *processing* of genetic data, biometric data, data concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions.

* For the purposes of this policy we use the term '*personal data*' to include '*sensitive personal data*' except where we specifically need to refer to *sensitive personal data*.

'*Supervisory authority*' means an independent public authority which is responsible for monitoring the application of data protection. In the UK the *supervisory authority* is the Information Commissioner's Office (ICO).

All of these definitions are italicised throughout this policy to remind the reader that they are defined terms.

Extraman Limited processes *personal data* in relation to its own staff, work-seekers and individual client contacts and is a *data controller* for the purposes of the Data Protection Laws. Extraman Limited has registered with the ICO and its registration number is Z4629685

Extraman Limited may hold and/or process *personal data* on individuals for the following purposes:

- Staff administration;
- Advertising, marketing and public relations
- Accounts and records;
- Administration and *processing* of work-seekers' *personal data* for the purposes of providing work-finding services, including *processing* using software solution providers and back office support;
- Administration and *processing* of clients' *personal data* for the purposes of supplying/introducing work-seekers.

Specific examples of when we might process your personal data:

We have to process your personal data in various situations during your recruitment, employment or engagement and even following termination of your employment or engagement. For example:

- to decide whether to employ or engage you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work in the UK;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct;
- to carry out a disciplinary or grievance investigation or complaints and disputes procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability;
- to monitor diversity and equal opportunities;
- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties;
- to pay you and provide pension and other benefits in accordance with the contract between us;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions;
- monitoring compliance by you, us and others with our policies and our contractual obligations;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us;
- to answer questions from insurers in respect of any insurance policies which relate to you;
- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;

- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure; and
- for any other reason which we may notify you of from time to time.

We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data, then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting Duncan Sykes, Director.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

We might process special categories of your personal data for the purposes detailed above which have an asterisk beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.
- We will only process information about criminal convictions this should be explained where we have specific legal authorisation

We do not take automated decisions about you, using your personal data or use profiling in relation to you, except where the automated/profiling decision:

- Is necessary for the entering into or performance of a contract between the Company and you;
- Is authorised by law; or
- You have given your explicit consent

1. The data protection principles

The Data Protection Laws require Extraman Limited acting as either *data controller* or *data processor* to process data in accordance with the principles of data protection. These require that *personal data* is:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and 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 for no longer than is necessary for the purposes for which the *personal data* are processed;
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; and that
7. The *data controller* shall be responsible for, and be able to demonstrate, compliance with the principles.

2. Legal bases for processing

Extraman Limited will only process *personal data* where it has a legal basis for doing so (see Annex A). Where Extraman Limited does not have a legal reason for *processing personal data* any processing will be a breach of the Data Protection Laws.

Extraman Limited will review the *personal data* it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this.

Before transferring *personal data* to any third party (such as past, current or prospective employers, suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back office support)), Extraman Limited will establish that it has a legal reason for making the transfer.

3. Privacy by design and by default

Extraman Limited has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all *processing* activities.

We are required to demonstrate that privacy considerations are embedded into all our processes and procedures. We complete documented data protection impact assessments on our processes and procedures to ensure we are compliant with the principles of GDPR. This is completed each time a policy or procedure is changed.

The types of measures that we implement includes:

- Data minimisation (i.e. not keeping the data longer than is necessary)

- Pseudonymisation (personal data which cannot be attributed to an individual without additional information. The information must be kept separately and is subject to technical and organisational measures to ensure the individual cannot be identified)
- Anonymisation (using separate keys/codes so that individuals cannot be identified)
- Cyber security

Extraman Limited shall provide any information relating to data *processing* to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. Extraman Limited may provide this information orally if requested to do so by the individual.

1. Privacy notices

Where Extraman Limited collects *personal data* from the individual, Extraman Limited will give the individual a privacy notice at the time when it first obtains the *personal data*.

Where Extraman Limited collects *personal data* other than from the individual directly, it will give the individual a privacy notice within a reasonable period after obtaining the *personal data*, but at the latest within one month. If Extraman Limited intends to disclose the *personal data* to a third party then the privacy notice will be issued when the *personal data* are first disclosed (if not issued sooner).

Where Extraman Limited intends to further process the *personal data* for a purpose other than that for which the data was initially collected, Extraman Limited will give the individual information on that other purpose and any relevant further information before it does the further *processing*.

2. Subject access requests

The individual is entitled to access their *personal data* on request from the *data controller*.

3. Rectification

The individual or another *data controller* at the individual's request, has the right to ask Extraman Limited to rectify any inaccurate or incomplete *personal data* concerning an individual.

If Extraman Limited has given the personal data to any third parties it will tell those third parties that it has received a request to rectify the *personal data* unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however Extraman Limited will not be in a position to audit those third parties to ensure that the rectification has occurred.

4. Erasure

The individual or another *data controller* at the individual's request, has the right to ask Extraman Limited to erase an individual's *personal data.*

If Extraman Limited receives a request to erase it will ask the individual if s/he wants his *personal data* to be removed entirely or whether s/he is happy for his or her details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise). Extraman Limited cannot keep a record of individuals whose data it has erased so the individual may be contacted again by Extraman Limited should Extraman Limited come into possession of the individual's *personal data* at a later date.

If Extraman Limited has made the data public, it shall take reasonable steps to inform other *data controllers* and *data processors processing* the *personal data* to erase the *personal data*, taking into account available technology and the cost of implementation.

If Extraman Limited has given the *personal data* to any third parties it will tell those third parties that it has received a request to erase the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however

Extraman Limited will not be in a position to audit those third parties to ensure that the rectification has occurred.

5. Restriction of *processing*

The individual or a *data controller* at the individual's request, has the right to ask Extraman Limited to restrict its *processing* of an individual's *personal data* where:

- The individual challenges the accuracy of the *personal data*;
- The *processing* is unlawful and the individual opposes its erasure;
- Extraman Limited no longer needs the *personal data* for the purposes of the *processing*, but the *personal data* is required for the establishment, exercise or defence of legal claims; or
- The individual has objected to *processing* (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of Extraman Limited override those of the individual.

If Extraman Limited has given the *personal data* to any third parties it will tell those third parties that it has received a request to restrict the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however Extraman Limited will not be in a position to audit those third parties to ensure that the rectification has occurred.

6. Data portability

The individual shall have the right to receive *personal data* concerning him or her, which he or she has provided to Extraman Limited, in a structured, commonly used and machine-readable format and have the right to transmit those data to another *data controller* in circumstances where:

- The *processing* is based on the individual's *consent* or a contract; and
- The *processing* is carried out by automated means.

Where feasible, Extraman Limited will send the *personal data* to a named third party on the individual's request.

7. Object to *processing*

The individual has the right to object to their *personal data* being processed based on a public interest or a legitimate interest. The individual will also be able to object to the *profiling* of their data based on a public interest or a legitimate interest.

Extraman Limited shall cease *processing* unless it has compelling legitimate grounds to continue to process the *personal data* which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

The individual has the right to object to their *personal data* for direct marketing.

8. Enforcement of rights

All requests regarding individual rights should be sent to the person whose details are listed in the Appendix.

Extraman Limited shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision making processes or profiling within one month of receipt of the request. Extraman Limited may extend this period for

two further months where necessary, taking into account the complexity and the number of requests.

Where Extraman Limited considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature Extraman Limited may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

9. Automated decision making

Extraman Limited will not subject individuals to decisions based on automated *processing* that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

- Is necessary for the entering into or performance of a contract between the *data controller* and the individual;
- Is authorised by law; or
- The individual has given their explicit *consent*.

Extraman Limited will not carry out any automated decision-making or *profiling* using the *personal data* of a child.

Reporting *personal data* breaches

All data breaches should be referred to the persons whose details are listed in the Appendix.

1. *Personal data breaches* where Extraman Limited is the *data controller*:

Where Extraman Limited establishes that a *personal data breach* has taken place, Extraman Limited will take steps to contain and recover the breach. Where a *personal data breach* is likely to result in a risk to the rights and freedoms of any individual Extraman Limited will notify the ICO.

Where the *personal data breach* happens outside the UK, Extraman Limited shall alert the relevant *supervisory authority* for data breaches in the effected jurisdiction.

2. *Personal data breaches* where Extraman Limited is the *data processor*:

Extraman Limited will alert the relevant *data controller* as to the *personal data breach* as soon as they are aware of the breach.

3. Communicating *personal data breaches* to individuals

Where Extraman Limited has identified a *personal data breach* resulting in a high risk to the rights and freedoms of any individual, Extraman Limited shall tell all affected individuals without undue delay.

Extraman Limited will not be required to tell individuals about the *personal data breach* where:

- Extraman Limited has implemented appropriate technical and organisational protection measures to the *personal data* affected by the breach, in particular to make the *personal data* unintelligible to any person who is not authorised to access it, such as encryption.
- Extraman Limited has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
- It would involve disproportionate effort to tell all affected individuals. Instead, Extraman Limited shall make a public communication or similar measure to tell all affected individuals.

All individuals have the following rights under the Human Rights Act 1998 (HRA) and in dealing with *personal data* these should be respected at all times:

- Right to respect for private and family life (Article 8).
- Freedom of thought, belief and religion (Article 9).
- Freedom of expression (Article 10).
- Freedom of assembly and association (Article 11).
- Protection from discrimination in respect of rights and freedoms under the HRA (Article 14).

If you have a complaint or suggestion about Extraman Limited's handling of *personal data* then please contact the person whose details are listed in the Appendix to this policy.

Alternatively you can contact the ICO directly on 0303 123 1113 or at https://ico.org.uk/global/contact-us/email/

List names of those responsible for:

- **adding, amending or deleting *personal data*:**

- Duncan Sykes, Director
- Adrian Gregory, Director
- Kim Trees, Director
- Gary Waller, Director
- Emma Wadding, Manager
- Tim Shiel, Senior Consultant
- Ben McCulloch, Senior Consultant

- **responding to subject access requests/requests for rectification, erasure, restriction data portability, objection and automated decision making processes and profiling:**

- Duncan Sykes, Director
- Adrian Gregory, Director
- Kim Trees, Director
- Gary Waller, Director
- Emma Wadding, Manager

- **reporting data breaches/dealing with complaints; and/ordetails of the Data Protection Officer where applicable:**

- Duncan Sykes, Director

Contact Details:

Email: duncan@extramanrecruitment.co.uk
Phone: 020 7373 3045

Annex A - The lawfulness of *processing* conditions for *personal data* are:

1. *Consent* of the individual for one or more specific purposes.
2. *Processing* is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract.
3. *Processing* is necessary for compliance with a legal obligation that the controller is subject to.
4. *Processing* is necessary to protect the vital interests of the individual or another person.
5. *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 *data controller*.
6. *Processing* is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the individual which require protection of *personal data*, in particular where the individual is a child.

a) The lawfulness of *processing* conditions for *sensitive personal data* are:

1. Explicit *consent* of the individual for one or more specified purposes, unless reliance on *consent* is prohibited by EU or Member State law.
2. *Processing* is necessary for carrying out data controller's obligations under employment, social security or social protection law, or a collective agreement, providing for appropriate safeguards for the fundamental rights and interests of the individual.
3. *Processing* is necessary to protect the vital interests of the individual or another individual where the individual is physically or legally incapable of giving *consent*.
4. In the course of its legitimate activities, *processing* is carried out with appropriate safeguards by a foundation, association or any other not-for-profit body, with a political, philosophical, religious or trade union aim and on condition that the *processing* relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without the *consent* of the individual.
5. *Processing* relates to *personal data* which are manifestly made public by the individual.
6. *Processing* is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
7. *Processing* is necessary for reasons of substantial public interest on the basis of EU or Member State law which shall be proportionate to the aim pursued, respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual.
8. *Processing* is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional and subject to the necessary conditions and safeguards.
9. *Processing* is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the individual, in particular professional secrecy.
10. *Processing* is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard fundamental rights and interests of the individual.

Annex B - How should you process personal data for the Company?

Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security and Data Retention policies.

The Company's person acting in this capacity, Duncan Sykes, Director, is responsible for reviewing this policy and updating the Company management on the Company's data protection responsibilities and any risks in relation to the processing of data.

The following details the key rules and good practice that apply to everyone in the Company that processes personal data and you may be subject to monitoring, inspection and risk assessment to ensure that these are being applied.

1. You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
2. You should not share personal data informally.
3. You should keep personal data secure and not share it with unauthorised people.
4. You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.
5. You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
6. You should use strong passwords.
7. You should lock your computer screens when not at your desk.
8. Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
9. Do not save personal data to your own personal computers or other devices.
10. Personal data should never be transferred outside the European Union except in compliance with the law and authorisation of Duncan Sykes, Director.
11. You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
12. You should not take personal data away from Company's premises without authorisation from your line manager or the Data Protection Officer
13. Personal data should be shredded and disposed of securely when you have finished with it.
14. You should ask for help from the Data Protection if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.
15. Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.
16. It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.