Lawson Clark

DATA PROTECTION POLICY

(and record of processing activities under Article 30 of the GDPR)

Adopted by Lawson Clark Limited on 18th May 2018 - Version 2

Contents

Introduction

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, **Lawson Clark Limited of 105 Bishopsgate, London EC2M 3UE ('the Company')** collects and processes both *personal data* and *sensitive personal data*. It processes such data in respect of various types of individual such as employees, workers, candidates for employment, agency workers, clients contacts, supplier contacts and vendor contacts.

This policy sets out how the Company implements the Data Protection Laws.

The reasons for *processing personal data* vary depending on the data collected and we explain our reasons in this policy and in privacy notices that may be issued to (i) our own employees, consultants or workers; (ii) to candidates for employment or agency workers; and (iii) to other categories of data subject.

We also explain in this policy, the measures in place to protect the security of *personal data* and *sensitive personal data*.

We only hold data for as long as is necessary for the purposes for which we collect it. We set out in this policy our practices regarding data retention and erasure.

The Company expects employees to observe the obligations regarding the *processing* of *personal data* and *sensitive personal data* as set out in this policy at all times.

If there are any queries in relation to this policy it should be directed to the Data Protection Manager who is John Pittman who is a Director of the Company and who can be contacted by phone on 020 7256 6666.

This document also serves as a record of our *processing* activities pursuant to Article 30 of the General Data Protection Regulation.

Definitions

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 personal 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* includes *sensitive personal data* and *pseudonymised personal data* but excludes anonymous data or data that has had the identity of an individual permanently removed. *Personal data* can be factual (e.g. date of

birth, address) or an opinion about that person and an indication of the intentions of us or others, in respect of that 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.

Data processing under the Data Protection Laws

1. What data do we process?

The Company processes *personal data* in relation to its own staff (employees, workers, consultants etc), work-seekers (candidates for employment and agency workers), individual client contacts and individual contacts within suppliers or vendors and is a *data controller* for the purposes of the Data Protection Laws. The Company has registered with the ICO and its registration number is Z8062417.

(a) Our own staff (employees, consultants and workers)

We will collect and use the following types of *personal data* about our own staff:

- your name and address;
- recruitment information such as that contained in your application form and CV, education history, employment history, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;

- your gender;
- your marital status and family details;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- attendance and absence records whether relating to sickness or injury, holiday or other reasons for absence (including but not limited to statutory types of leave);
- your bank details and information in relation to your tax status including your national insurance number;
- payroll records;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training records;
- accident records;
- expenses claims;
- electronic information and hard copy information in relation to your use of IT systems and telephone systems; and
- any other category of personal data which we may notify you of from time to time.

We may collect and use the following types of *sensitive personal data* about our own staff:

- information about your health.

(b) Candidates for employment to whom we provide work finding services

When a candidate asks us to help them find employment with a third party, then we may collect and process the following types of *personal data*:

- your name and address;
- recruitment information such as that contained in your application form and CV, education history, references, qualifications, language skills, and membership of any professional bodies and details of any pre-employment assessments;
- your contact details;
- information relating to your employment history, previous roles held;
- details of roles applied for, employers approached, interviews undertaken, roles offered;
- the contract terms of any potential offer and of an accepted role;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work in the UK;
- test scores and results in respect of typing, grammar, spelling and use of Microsoft Word; and
- any other category of personal data which we may notify you of from time to time.

We may collect and use the following types of *sensitive personal data* about candidates:

- information about your health.

We *pseudonymise* candidate data by allocating a reference ID number to all registered candidates.

(c) Agency workers

The *personal data* we collect and process in relation to agency workers is the same as that which we collect in respect of candidates for employment, but in addition, we will also process the following types of *personal data*:

- gender and date of birth;
- methods of travel and travelling times;
- details of assignments applied for, interviewed for and placed in, including dates and feedback;
- details of holidays planned and taken;
- attendance and absence records whether relating to sickness or injury, holiday or other reasons for absence;
- bank details and information in relation to tax status including national insurance number;
- timesheets and payroll/payment records; and
- pension information.

(d) Clients

We collect and process *personal data* relating to individual contacts within client entities with whom we negotiate and discuss the provision of our recruitment services, to whom candidates and agency workers are introduced or supplied and to whom we submit invoices and contact for credit control purposes.

(e) Suppliers and vendors

We collect and process *personal data* relating to individual contacts within supplier or vendor entities with whom we negotiate and discuss the provision of goods and services and payment for such goods and services.

2. From where do we obtain personal data?

We primarily obtain *personal data* from the individual concerned.

We may also obtain *personal data* in respect of our own staff, candidates and agency workers from referees, whose details you will have provided us with. We may also obtain *personal data* in respect of candidates and agency workers from third party job websites or business or social media networking sites, which the individual would have provided to such sites. This is not a standard practice but may be used on occasion.

We endeavour to collect and process only such data as is relevant to our stated purposes for *processing* and to limit our *processing* of *personal data* to such purposes.

3. The data protection principles

The Data Protection Laws require the Company 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.

4. Legal bases for processing

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

The Company 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.

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)), the Company will establish that it has a legal reason for making the transfer.

5. What are our reasons for processing personal data?

We will use *personal data* of our staff, candidates for employment and agency workers as follows:

- performing the contract of employment (or for services) between us;

- complying with any legal obligation, including but not limited to prevailing employment law such as the Employment Rights Act 1996, the Equality Act 2010, the Working Time Regulations 1998; prevailing law governing the prevention of illegal working in the UK; law specific to the regulation of the recruitment industry such as the Employment Agencies Act 1973, the Conduct of Employment Agencies and Employment Businesses Regulations 2003; the Agency Workers Regulations 2010; prevailing tax law; or

- if it is necessary for our legitimate interests (or for the legitimate interests of someone else), e.g. in order to our provide work finding services. However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this *processing*. See details of your rights in the section entitled "Rights of the Individual" below.

If you choose not to provide us with certain *personal data* you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

We will use *personal data* of client contacts and supplier or vendor contacts as follows:

- performing the contract for services between us; or

- if it is necessary for our legitimate interests, e.g. in order for us to provide you with our recruitment services or to supply an agency worker in the case of our clients; or in our to purchase your services in the case of our suppliers or vendors.

We can process *personal data* for these purposes without the individual's knowledge or *consent*. We will not use *personal data* for an unrelated purpose without informing the data subject about it and the legal basis that we intend to rely on for *processing* it.

6. When will we process personal data?

In relation to our staff, candidates for employment and agency workers, we have to process *personal data* in various situations during recruitment, employment (or engagement) and even following termination of employment (or engagement).

For example, in relation to our own staff; examples of when we may process *personal data* may include:

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and to execute our obligations under 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 procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to the workplace or role because of a disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of the Company, of you, our other staff and others;
- to monitor and protect the health and safety of you, our other staff and third parties*;
- to pay you and provide pension and other benefits in accordance with the contract between us*;
- paying tax and national insurance;
- education, training and development requirements and provision;
- making decisions about your continued employment or termination thereof;
- to provide a reference upon request from another employer;
- 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*;
- 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.

In relation to candidates for employment with our clients, we may use *personal data* when we are assessing whether you are suitable for a client vacancy, to inform the client of your suitability, to arrange interviews, as part of discussing the terms of any offer of employment and otherwise to provide our services to both you and relevant clients. We may need to retain data after we have found employment for you to comply with prevailing law and to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure.

In relation to agency workers that we place with end user clients, examples of when we may process *personal data* may include:

- to decide whether to engage you;

- to decide how much to pay you, and to execute our obligations under 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;
- reviewing your performance*;
- to determine whether reasonable adjustments to a workplace or role because of a disability may be required*;
- to monitor diversity and equal opportunities*;
- 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 a future employer;
- monitoring compliance by you 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*;
- 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.

Again, we will need to retain some of this data even after you have ceased to perform assignments for us.

In relation to client contacts, we process *personal data* when we provide our recruitment services to the client.

In relation to supplier or vendor contacts, we process *personal data* when we order and accept goods and services from such parties.

7. Sensitive personal data

We will only process *sensitive personal data* in certain situations in accordance with the law. We do not process *sensitive personal data* of client, supplier or vendor contacts. We may find it necessary to process *sensitive personal data* in relation to our own staff, candidates for employment or agency workers. We can do so if we have your explicit *consent*. If we asked for your *consent* to process *sensitive 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 the Data Protection Manager.

We do not need your *consent* to process *sensitive 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 in section 5 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, however this will be on an anonymous basis and you will not be identifiable from that information, if given to us, therefore will not be identifiable as your *personal data*;
- 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.

8. Who will we share your personal data with?

In relation to our own staff, we will share *personal data* with NEST, our auto enrolment pension provider for the purposes of administrating your pension.

In relation to candidates for employment with our clients, to whom we provide work finding services, we will share your *personal data* with clients who may be suitable potential employers. We will notify you first before we send your *personal data* to any of our clients.

In relation to agency workers that we place with clients, we will share your *personal data* with clients who have work assignments to be filled by an agency worker where such assignment is suitable for you. We will notify you first before we send your *personal data* to any of our clients. We share your data with NEST, our auto enrolment pension provider for the purposes of administrating your pension.

In relation to our client contacts, we will share contact data with candidates and agency workers that you have expressed an interest in hiring.

We do not share *personal data* relating to suppliers or vendors.

We do not send *personal data* outside the European Economic Area. If this changes the data subject will be notified of this and the protections which are in place to protect the security of the data will be explained.

9. Impact assessments

We understand that where a type of *processing* (in particular using new technology), taking into account the nature, scope, context and purposes of *processing* is likely to result in a high risk to the rights and freedoms of an individual, we are obliged to carry out an assessment of the impact of the envisaged *processing* operations on the protection of *personal data*.

At present, the Company does not engage in *processing* which we believe is likely to result in a high risk to the rights or freedoms of any individual.

Data security

We appreciate that *personal data* must be secured by appropriate technical and organisational measures against unauthorised or unlawful *processing* and against accidental loss, destruction or damage. We have and will continue to develop, implement and maintain safeguards appropriate to the size and scope of our business, our available resources and taking into account the amount of *personal data* that we handle. We will regularly evaluate and test the effectiveness of those safeguards to ensure to ensure security of our *processing* of *personal data*. All staff are responsible for protecting *personal data* that we hold.

1. Data locations

Our IT system is housed in our own server located in London. The majority of the *personal data* we collect is saved to this server. Manual records are kept securely also in London.

2. Privacy by design and by default

The Company has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all *processing* activities. This includes implementing measures such as:

- data minimisation (i.e. not keeping data for longer than is necessary) (see "Data retention and erasure" section below);
- anonymization (as referred to above, we only accept anonymised *personal data* in relation to diversity monitoring); and
- cyber security.

We are also investigating pseudonymisation of candidate and agency worker data to increase security of such data with the intention of introducing this in due course.

Specific security measures include the following:

- All data collected via our website is transmitted to from the user device over a TLS encrypted connection that has been secured with an SSL Certificate supplied by Digicert. Encryption is enforced.
- Where possible, all internet email is sent and received over a TLS encrypted connection that has been secured with an SSL Certificate supplied by Digicert.

Data retention and erasure

The Company's approach to retaining *personal data* is to ensure that it complies with the data protection principles referred to above and in particular to ensure that:

- The extent of *personal data* collected and processed is regularly reviewed to ensure that they remain adequate, relevant and limited to what is necessary to facilitate the purpose for which it is collected.
- *Personal data* is kept secure and are protected against unauthorised or unlawful *processing* and against accidental loss, destruction or damage.
- When records are destroyed, whether held as paper records or in electronic format, the Company will ensure that they are safely and permanently erased.

We retain personal information following recruitment exercises to demonstrate, if required, that individuals have not been discriminated against on prohibited grounds and that recruitment exercises are conducted in a fair and transparent way.

Information relating to successful candidates, agency workers and our own staff will be retained for such period as is necessary for the working relationship and, where applicable, that required by law.

Information relating to clients, vendors and suppliers will be held for so long as our business relationship is active and for a period thereafter.

Retention and destruction of *personal data* will take place in accordance with the Data Retention and Destruction Policy which is available on request from John Pittman on 020 7256 6666

Record keeping

The Data Protection Laws require us to keep full and accurate records of our data *processing* activities.

Those records should include as a minimum, the name and contact details of the *data controller*, clear descriptions of the *personal data* types, data subject types, *processing* activities, *processing* purposes, third party recipients, storage locations, *personal data* transfers, data retention periods and a description of our security measures.

We have recorded this information in this policy document and have based this policy document on a data mapping exercise tracking our data flows.

All of our staff have a responsibility to track *personal data* and its *processing* and to keep records of any specific *consents* obtained.

Rights of the individual

The Company 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. The Company may provide this information orally if requested to do so by the individual.

Any request received by our staff in which an individual seeks to assert any of the rights referred to below should be immediately referred to the Data Protection Manager.

1. Privacy notices

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

Where the Company 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 the Company 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 the Company intends to further process the *personal data* for a purpose other than that for which the data was initially collected, the Company 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 the Company to rectify any inaccurate or incomplete *personal data* concerning an individual.

If the Company 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 the Company 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 the Company to erase an individual's *personal data.*

If the Company 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). The Company cannot keep a record of individuals whose data it has erased so the individual may be contacted again by the Company should the Company come into possession of the individual's *personal data* at a later date.

If the Company 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 the Company 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 the Company will not be in a position to audit those third parties to ensure that the erasure has occurred.

An individual's right to require erasure may not apply to the extent that processing is necessary:

- For exercising the right of freedom of expression and information.
- For compliance with a legal obligation which requires processing by the Company, or for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the Company.
- For the establishment, exercise or defence of legal claims.

In the event we believe that continued processing is necessary and we are unable to effect erasure, we will explain our reasons.

5. Restriction of processing

The individual or a *data controller* at the individual's request, has the right to ask the Company 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;
- The Company 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 the Company override those of the individual.

If the Company 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 the Company will not be in a position to audit those third parties to ensure that the restriction 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 the Company, 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, the Company 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.

The Company 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 Data Protection Manager.

The Company 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. The Company may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where the Company considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature the Company 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

The Company 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*.

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

Reporting personal data breaches

All *personal data breaches* should be referred to the Data Protection Manager immediately.

1. Personal data breaches where the Company is the data controller:

Where the Company establishes that a *personal data breach* has taken place, the Company 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 the Company will notify the ICO within 72 hours.

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

2. Personal data breaches where the Company is the data processor:

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

The Company will not be required to tell individuals about the *personal data breach* where:

- The Company 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.
- The Company 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, the Company shall make a public communication or similar measure to tell all affected individuals.

The Human Rights Act 1998

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).

Training

The Company will assess training requirements in respect of Data Protection Laws on an ongoing basis and provide such training as it believes is appropriate to its staff.

Review periods

The Company will ensure that it reviews what *personal data* it processes, how it processes it and why on an ongoing basis.

This policy and the data protection practices that are referred to in it will be reviewed by the Company regularly and not less than annually. The next review will take place in April 2019.

Complaints

If you have a complaint or suggestion about the Company's handling of *personal data* then please contact John Pittman who is a Director of the Company on 020 7256 6666.

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

Annex A

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.

b) 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.