GDPR POLICY

Purpose	Our GDPR Policy & Procedure covers the entire General Data Protection Regulation requirements and standards. This document enables all employees within our business to demonstrate compliance, evidence their commitment to data protection and mitigate processing risks
Company	In-house Recruitment
Author	Natasha Preocanin, Managing Director
Last Updated	22nd April 2020
Version	V 1.4

To Note: Whilst the GDPR applies directly to the UK, our existing DPA needs to be updated to implement the GDPR, enable the UK to exercising derogations in the GDPR, introduce specific provisions (where applicable) and prepare for Brexit. The Government has introduced the Data Protection Bill to the House of Lords (on 13 September 2017), which will update UK data protection laws once passed. Once the Data Protection Bill is enacted into UK law, our GDPR policy will be updated with any additional provisions and/or exemptions.

1. POLICY STATEMENT

In-house Recruitment needs to collect personal information about the people we deal with to effectively and compliantly carry out our everyday business functions and activities and to provide the products and services defined by our business type. This information can include (but is not limited to), name, address, email address, data of birth, IP address, identification number, private and confidential information, sensitive information and bank details.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the General Data Protection Regulation, UK data protection law and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

In-house Recruitment has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the GDPR and its principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and safety of personal and/or special category data belonging to the individuals with whom we deal is paramount to our company ethos and In-house Recruitment adheres to the GDPR and its associated principles in every process and function.

We are proud to operate a 'Privacy by Design' approach and aim to be proactive not reactive; assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

2. PURPOSE

The purpose of this policy is to ensure that In-house Recruitment is meeting its legal, statutory and regulatory requirements under the GDPR and to ensure that all personal and special category information is safe, secure and processed compliantly whilst in use and/or being stored and shared by us. We are dedicated to compliance with the GDPR's principles and understand the importance of making personal date safe within our business.

To this end, we provide our staff with frequent training sessions, compliance updates and assessments regarding the GDPR rules, principles and guidelines to ensure their knowledge and understanding of this area is adequate, effective and relevant to their role. The measures in this policy are compliant with the GDPR rules and as such, support our staff and give them the confidence and competence to process personal information compliantly.

The GDPR includes provisions that promote accountability and governance and as such In-house Recruitment has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data.

2.1 SCOPE

The policy relates to all staff (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with In- house Recruitment in the UK or overseas) within the organisation and has been created to ensure that staff deal with the area that this policy relates to in accordance with legal, regulatory, contractual and business expectations and requirements.

2.2 DEFINITIONS

Anonymisation: A process that transforms identifiable data (personal) into non-identifiable data (non-personal). In the context of the UK Data Protection Act (DPA), anonymisation is a process that tackles the removal of information from a data set that can indirectly identify an individual or be combined with other data to identify an individual. In scientific circles, there are various types of anonymisation that render data more or less non-personal and therefore more or less useful.

Anonymisation (Absolute): An anonymisation technique whereby the resulting data has zero risk of re-identification under any circumstances. No information or insights can be extracted from this data meaning its utility is limited.

Anonymisation (Formal): A process that removes direct identifiers from the data but doesn't remove indirect identifiers. This can include replacing direct identifiers with pseudonyms

Anonymisation (Statistical / functional): Anonymisation techniques that take into account the statistical risk of re-identification and the context within which the data is being used. These techniques seek to balance the risk of disclosure of personal data with the usefulness of the resulting data set.

Authentication: The process by which a person or entity proves that they are who they claim to be.

Binding Corporate Rules (BCRs): A set of internal rules put in place to allow multinational companies and organisations to transfer personal data that they control from the EU to their affiliates outside the EU but within the organisation.
Biometric Data: Any personal data relating to the physical, physiological, or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images.

Breach notifications: UK organisations will be required to report data breaches to the ICO within 72 hours of becoming aware of it. In serious cases, where customer data is at serious risk, the individuals concerned must be notified.
Confidentiality

Measures undertaken to prevent sensitive information from reaching unintended recipients whilst enabling the correct parties to access it. Whereas privacy typically relates to personal data, confidentiality is used in conjunction with non-personal data, such as company financial statements, intellectual property or other commercially sensitive information.

Consent: Informed, unambiguous, freely given, specific, and explicit consent by statement or action from the data subject to have data relating to him or her processed.

Cross-Border Processing: The processing of personal data when the controller or processor is established in more than one Member State and the data processing takes place in more than one Member State, or processing activities that take place in a single establishment in the Union, but that affects data subjects from more than one Member State.

Ciphertext: Encrypted text. This term is often used in the context of cryptography to refer to (plain) text that has been encrypted.

The Data Protection Act: Implemented by the UK government in 1998 to control how personal information is used by organisations and give legal rights to individuals.

Data Protection Authority: National authorities that enforce the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Data controller: A legal individual, public authority, agency or other body which, alone or jointly with others, determines the purposes and methods of processing personal data.

Data Entity: A unit of data that constitutes a fact, for instance a name, social security number, telephone number etc.

Data Masking: A method of creating a structurally similar but inauthentic version of an organisation's data that can be used for software testing and user training.

Data processor: A legal individual, public authority, agency, or body which processes personal data on behalf of the controller.

Data Protection Officer: An expert on data privacy who works independently to ensure that an organisation is adhering to the policies and procedures in the GDPR.

The Data Protection Act 1998 (DPA): An Act of Parliament of the United Kingdom of Great Britain and Northern Ireland to make provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The DPA is the main piece of legislation that governs the protection of personal data in the UK.

Data Subject: A data subject is a natural, living person who can be identified by the data stored whose personal data is processed by a controller or processor.

Delegated Acts: Non-legislative acts enacted in order to supplement existing legislation and provide criteria or clarity.

Directive: A legislative act that sets out a goal that all EU countries must achieve through their own national laws.

Encryption: The process of disguising a message or data in such a way as to hide its substance.

Encrypted Data: The protection of personal data through technological measures to ensure that the data is only accessible/readable by those with specified access.

Genetic Data: Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the health or physiology of the individual.

Identifiable data: Data that contains indirect identifiers.

Identified data: Data that contains direct identifiers.

Identifier (Direct): Any data item that, on its own, could uniquely identify an individual. It is sometimes referred to as a direct identifier or formal identifier, examples of which include a data subject's name, address and unique reference numbers e.g. their social security number or National Health Service number.

Identifier (Indirect): A data item that can be used with other available information to identify an individual. It can also include a combination of items of information that can together identify an individual.
Integrity
Accuracy and consistency of data; freedom of data from corruption.

Identifier (Indirect): A data item that can be used with other available information to identify an individual. It can also include a combination of items of information that can together identify an individual.

Personal Data: Any information related to an identified or identifiable natural person or 'Data Subject' that can be used to directly or indirectly identify the person.

Personal Data Breach: A breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Personal Sensitive Data: Sensitive information related to an identified or identifiable natural person or 'Data Subject' that can be used to directly or indirectly identify the person. Examples include but are not limited to; Sexual orientation, Religious Beliefs, Political memberships.

Privacy by Design: An approach to projects that designs privacy and data protection

compliance from the start, rather than as an afterthought.
Privacy Impact Assessment (PIA): A tool that is used to identify and reduce the privacy risks of a project. A PIA helps reduce the risk of misuse of personal data processed and can help to design more efficient and effective processes for handling personal data.

Processing: Any operation performed on personal data, such as including collection, use, recording, etc.

Profiling: Automated processing of personal data which enables aspects of an individual's personality or behaviour, interests, and habits to be determined, analysed and predicted.

Pseudonymization: A process to make personal data no longer attributable to a single data subject without the use of additional data. Additional data must be separate to ensure non-attribution.

Recipient: An entity to which the personal data is disclosed.

Representative: Any person in the Union explicitly designated by the controller to be addressed by the supervisory authorities.

Right to Access: Also known as 'Subject Access Right'. Data Subjects are entitled to the have access to and information about the personal data that a controller has concerning them.

Right to Erasure: Also commonly known as the 'right to be forgotten'. GDPR enhances this concept to give individuals more power to request the removal or deletion of their personal data. Depending on the circumstances, organisations will also have to remove backups and archived data, as well as information shared with third parties.

Right to Portability: Allows individuals to obtain their personal data and reuse it elsewhere if they wish to. Organisations are obliged to comply with requests providing the information in question meets a specific set of criteria and must be provided in a commonly used and readable format.

Supervisory Authority: A public authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data. An organisation will contact them for compliance activity such as registering a data protection officer, notifying a risky processing activity or notifying a data security breach.

Third Country: Recipients located outside the EEA.

Trilogues: Informal negotiations between the European Commission, the European Parliament, and the Council of the European Union. They are usually held following the first readings of proposed legislation to help move to a quicker agreement on how the text can be adopted.

3. DATA PROTECTION BACKGROUND

The UK initially had The Data Protection Act 1984 in place to regulate the use of processed information that related to individuals. However, in 1995 the introduction of EU Directive 95/46/EC which set aims and requirements for member states on the protection of personal data when processing or sharing, meant an updated Act was

required.

The UK subsequently developed and enacted The Data Protection Act 1998 (DPA) to ensure that British law complied with the EU Directive and to provide those with obligations under the Act, with updated rules, requirements and guidelines for processing and sharing personal data.

2018 marks the 20th anniversary of the DPA enactment and whilst there have been periodical additions or alterations to the Act, technology has advanced at a far faster rate, necessitating new regulations for the current digital age. The past 20 years has also seen a vast increase in the number of businesses and services operating across borders, further highlighting the international inconsistency in Member States individual data protection laws.

For this reason, in January 2012, the European Commission proposed a new regulation applying to all EU Member States and bringing a standardised and consistent approach to the processing and sharing of personal information across the EU.

4. GENERAL DATA PROTECTION REGULATION (GDPR)

The General Data Protection Regulation (GDPR) (EU)2016/679) was approved by the European Commission in April 2016 and will apply to all EU Member States from 25th May 2018. As a 'Regulation' rather than a 'Directive', its rules apply directly to the Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As In-house Recruitment processes personal information regarding individuals (data subjects), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with the GDPR and its principles.

Information protected under the GDPR is known as “personal data” and is defined as: -

“Any information relating to an identified or identifiable natural person; 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.”

In-house Recruitment ensures that even greater care and attention is given to personal data falling within the GDPR’s ‘special categories’ (previously referred to under the DPA as sensitive personal data), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the ‘Special categories of Personal Data’ the GDPR advises that: -

Processing of 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 for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.

The GDPR regulates the processing of personal data, which includes organisation, altering, adapting, retrieving, consulting on, storing, using, disclosing, transmitting, disseminating or destroying any such data. As In-house Recruitment uses personal data in one or more of the above capacities, we have put into place robust measures, policies, procedures and controls

concerning all aspects of personal data handling.

4.1 THE GDPR PRINCIPLES

Article 5 of the GDPR requires that personal data shall be: -

1. Processed lawfully, fairly and in a transparent manner in relation to individuals
2. 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
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Accurate and, where necessary, 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 in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 GDPR in order to safeguard the rights and freedoms of individuals
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

Article 5(2) requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles and requires that we show how we comply with the principles, detailing and summarising the measures and controls that we have in place to protect personal information and mitigate the risks of processing.

4.2 NATIONAL DATA PROTECTION LAW

To ensure that there is no confusion between the EU General Data Protection Regulation (GDPR) and the UK's existing Data Protection Act 1998 (DPA) after May 2018 and in preparation for Brexit, the Government introduced the Data Protection Bill to the House of Lords on 13 September 2017, which will implement the GDPR and update UK data protection laws once passed. The Bill will also enable the UK to exercise derogations in the GDPR & introduce more specific provisions where applicable.

4.3 THE INFORMATION COMMISSIONERS OFFICE (ICO)

The Information Commissioners Office (ICO) is an independent regulatory office who report directly to Parliament and whose role it is to uphold information rights in the public interest. The legislation they have oversight for includes: -

- The Data Protection Act 1998 (pre-25th May 2018)
- The Data Protection Bill [awaiting name of new enacted DP Law once finalised]
- General Data Protection Regulation (post-25th May 2018)
- The Privacy and Electronic Communication (EU Directive) Regulations 2003
- Freedom of Information Act 2000
- The Environmental Information Regulations 2004

ICO's mission statement is “to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals” and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

Under the GDPR the ICO, as the UK's data protection authority (Supervisory Authority), will have a similar role as before when it comes to oversight, enforcement and responding to complaints with regards to the GDPR and those firms located solely in the UK.

However, where an organisation is based in more than one Member State and/or where cross border processing takes place, a lead Supervisory Authority will enforce the GDPR requirements in consultation with any associated Supervisory Authority. Under the GDPR, the 'lead' is determined by the location of the 'main establishment'.

In-house Recruitment are registered with ICO and appear on the Data Protection Register as a controller and a processer of personal information.

Our Data Protection Registration Number is A8255507 5. OBJECTIVES

We are committed to ensuring that all personal data obtained and processed by In-house Recruitment is done so in accordance with the GDPR and its principles, along with any associated regulations and/or codes of conduct laid out by the Supervisory Authority and local law. We are dedicated to ensuring the safe, secure, ethical and transparent use of all personal data and to uphold the highest standards of data processing.

In-house Recruitment uses the below objectives to meet the regulatory requirements of the GDPR and to develop measures, procedures and controls for maintaining and ensuring compliance.

In-house Recruitment ensures that: -

- We protect the rights of individuals with regards to the personal information known and held about them by In-house Recruitment in the course of our business.
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the GDPR.
- Every business practice, task and process carried out by In-house Recruitment is monitored for compliance with the GDPR and its principles.
- Data is only obtained, processed or stored when we have met the lawfulness of processing requirements
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested.
- All employees (including new starters and freelancers/consultants etc.) are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the GDPR principles, regulations and how they apply to our business and services.
- Customers feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the GDPR.
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the GDPR and to identify gaps and non-compliance before they become a risk.
- We monitor the Supervisory Authority, European Data Protection Board (EDPB) and GDPR news and updates, to stay abreast of updates, notifications and additional requirements.
- We have robust and recorded Complaint Handling and Breach Incident controls and procedures in place for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection.

- We have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program utilises this policy and procedure and the GDPR itself to ensure continued compliance.
- We provide clear lines of reporting and supervision with regards to data protection compliance.
- Develop and maintain strict and robust DPA procedures, controls and measures to ensure continued compliance with the Act.
- We store and destroy all personal information, in accordance with the GDPR timeframes and requirements.
- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

5.1 DATA PROTECTION OFFICER

In-house Recruitment have appointed a DPO due to the nature of our business activities and/or the services that we provide. We have utilised our existing due diligence measures and procedures, along with extensive employee screening methods, to ensure that the appointed Data Protection Officer has been designated on the basis of their professional qualities.

We provide support, training, mentoring and CPD for the DPO, to ensure that they have an expert knowledge of data protection law, practices and principles and the ability to fulfil the tasks referred to in Article 39 of the GDPR. The DPO reports to the highest level of management (TBD) and provides adequate and effective management information on the compliance, measures, controls, reviews, gaps and improvement actions plans.

The DPO is fully informed that their role in relation to data protection is bound by secrecy and confidentiality and they have completed a Confidentiality Agreement which is signed and held on file. Where our DPO fulfils other tasks and duties, we have carried out a risk-assessment to ensure that those tasks and duties do not result in a conflict of interests.

In-house Recruitment are registered with the Supervisory Authority and appear on the Data Protection Register as a controller and/or processer of personal information. The DPO and their contact details have been published on this register, as well as being provided directly to the Supervisory Authority.

5.1.1 DUTIES OF THE DATA PROTECTION OFFICER

The Data Protection Officer has assumed the below duties in compliance with Article 39 of the GDPR: -

- To inform and advise In-house Recruitment and any employees carrying out processing, of their obligations pursuant to the GDPR, the Supervisory Authorities guidelines and any associated data protection provisions
- To monitor compliance with the GDPR, associated data protection provisions In-house Recruitment own data protection policies, procedures and objectives
- To oversee the assignment of responsibilities, awareness-raising and training of staff involved in processing operations
- To carry out and review audits of the above-mentioned policies, procedures, employee duties and training programs
- To cooperate with the Supervisory Authority where required
- To act as the point of contact for the Supervisory Authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult,

where appropriate, with regard to any other matter
- In accordance with Article 35 (type of processing is likely to result in a high risk to the rights and freedoms of natural persons), the DPO will provide advice where requested with regards to any data protection impact assessment and monitor its performance pursuant
- Have due regard to, and be aware of, the risk associated with processing operations, considering the nature, scope, context and purposes of processing

5.1.2 DESIGNATED DATA PROTECTION OFFICER

NAME: Will Russell
POSITION: Co-founder
ADDRESS: 4th floor, 10 Lower Thames Street
EMAIL: hello@inhouserecruitment.co.uk
TEL: 0203 968 8858

5.1.3 DEPUTY DATA PROTECTION OFFICER

NAME: Mark Lennox
POSITION: Co-founder
ADDRESS: 4th floor, 10 Lower Thames Street
EMAIL: mark@inhouserecruitment.co.uk
TEL: 0203 968 8858

6. GOVERNANCE PROCEDURES

6.1 ACCOUNTABILITY & COMPLIANCE

Due to the nature, scope, context and purposes of processing undertaken by In-house Recruitment, we carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have also implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the GDPR and any codes of conduct that we have obligations under.

We can demonstrate that all processing activities are performed in accordance with the GDPR and that we have in place robust policies, procedures, measures and controls for the protection of data. We operate a transparent workplace and work diligently to guarantee and promote a comprehensive and proportionate governance program.

We operate a top-down approach to data protection and ensure that every employee within the company is knowledgeable about and has access to the GDPR requirements, its principles, related codes of conduct and out internal policies, measures and training documents. Staff will be frequently tested to assess their level competency and understanding of the data protection regulations and to demonstrate our commitment to protecting the information that we process.

Our main governance objectives are to: -

• Educate our senior management and employees about the requirements under the GDPR and the possible impact of non-compliance

- Provide a dedicated and effective data protection training program for all staff
- Identify key senior stakeholders to support the data protection compliance program

- Allocate responsibility for data protection compliance and ensure that the designated person has sufficient access, support and budget to perform the role
- Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organisational measures that In-house Recruitment has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated policies (e.g. Training Policy, Audit Procedures etc). These measures include: -

Data Protection (GDPR) Policy & Procedure

- Staff Training & Development Policy
- Internal Audits & Monitoring Policy & Procedures
- Information Security Policy & Procedures
- Outsourcing Policy & Due Diligence Procedures
- Clear Desk Policy
- Remote Access Policy
- Record Processing Activities
- Information Audit & Personal Data Register
- Appointed Data Protection Officer
- Business Continuity Plan & Daily Data Backups

6.1.1 PRIVACY BY DESIGN

We operate a 'Privacy by Design' approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We therefore have additional measures in place to adhere to this ethos, including: -

Data Minimisation

Under Article 5 of the GDPR, principle (c) advises that data should be 'limited to what is necessary', which forms the basis of our minimal approach. We only ever obtain, retain, process and share the data that is essential to carry out our services and legal obligations and we only keep if for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the GDPR.

Measures to ensure that only the necessary data is collected includes: -

- Electronic collection (i.e. forms, website, surveys etc) only have the fields that are relevant to the purpose of collection and subsequent processing. We only include 'optional' fields where is it made clear that adding these details will enable us to provide an improved service in a clear manner
- Physical collection (i.e. face-to-face, telephone etc) is supported using scripts and internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected
- We have SLA's and bespoke agreements in place with third-party controllers who send us personal information (either in our capacity as a controller or processor). These state that only relevant and necessary data is to be provided as it relates to the processing activity we are carrying out.
- We have documented destruction procedures in place where a data subject or third-party provides us with personal information that is surplus to requirement.

Pseudonymisation- RL and PO to advise outside of employee data

We utilise pseudonymisation where possible to record and store personal data in a way that ensures data can no longer be attributed to a specific data subject without the use of separate additional information (personal identifiers). Encryption and partitioning is also used to protect the personal identifiers, which are always kept separate from the pseudonymised data sets.

When using pseudonymisation, we ensure that the attribute(s) being removed and replaced, are unique and prevent the data subject from being identified through the remaining markers and attributes. Pseudonymisation means that the data subject is still likely to be identified indirectly and as such, we use this technique in conjunction with other technical and operational measures of risk reduction and data protection.

Encryption

Although we class encryption as a form of pseudonymisation, we also utilise it as a secondary risk prevention measure for securing the personal data that we hold. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

We utilise encryption via secret key for transferring personal data to any external party and provide the secret key in a separate format. Where special category information is being transferred and/or disclosed, the Data Protection Officer is required to authorise the transfer and review the encryption method for compliance and accuracy.

Restriction

Our Privacy by Design approach means that we use company-wide restriction methods for all personal data activities. Restricting access is built into the foundation of In-house Recruitment processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information. Special category data is restricted at all levels and can only be accessed by our data protection team.

Hard Copy Data

It is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options (i.e. GP/Occupational Health information). Where this is necessary, we will utilise a tiered approach to minimise the information we hold and/or the length of time we hold it for.

Steps include: -

- In the first instance, we always ask the initial data controller to send copies of any personal information records directly to the data subject initially
- Where step 1 is not possible or feasible, we will obtain a copy of the data and if applicable redact to ensure that only the relevant information remains (i.e. when the data is being passed to a third-party for processing and not directly to the data subject)
- When only mandatory information is visible on the hard copy data, we utilise electronic formats to send the information to the recipient to ensure that encryption methods can be applied (i.e. we do not use the postal system as this can be intercepted).
- Recipients (i.e. the data subject, third-party processer) are re-verified and their identity and contact details checked

- The Data Protection Officer authorises the transfer and checks the file(s) attached and encryption method and key
- Once confirmation has been obtained that the recipient has received the personal information, where possible (within the legal guidelines and rules of the GDPR), we destroy the hard copy data and delete the sent message
- If for any reason a copy of the paper data must be retained by In-house Recruitment, we use a physical safe to store such documents as oppose to our standard archiving system

6.1.2 RESTRICTED ACCESS & CLEAR DESK POLICY

In-house Recruitment may on occasions and at its discretion, place all or part of its files onto a secure computer with restricted access to all/some personnel data. When implemented, access to personal information will only be granted to the person/department that has a specific and legitimate purpose for accessing and using such information.

In-house Recruitment operates a zero-tolerance Clear Desk Policy and does not permit personal data to be left unattended on desks or in meeting rooms, or in visible formats, such as unlocked computer screens or on fax machines, printers etc. Access to areas where personal information is stored (both electronic and physical) are on a restricted access basis with secure controlled access functions throughout the building. Only staff authorised to access data or secure areas are able to do so. All personal and confidential information in hard copy is stored safely and securely.

6.1.3 INFORMATION AUDIT

To enable In-house Recruitment to fully prepare for and comply with the GDPR, we have carried out a company-wide data protection information audit to better enable us to record, categorise and protect the personal data that we hold and process.

The audit has identified, categorised and recorded all personal information obtained, processed and shared by our company in our capacity as a controller and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Access level (i.e. full, partial, restricted etc)

We (alongside our partner SOLA) have also carried out an information audit in our capacity as a data processor, having identified, categorised and recorded all personal information that we process on behalf of a controller (or joint controllers). Refer to the ‘Processing Activities’ section of this policy for more information.

The Information Audit is an essential compliance tool and should be carried out. The format of the audit register will depend on how much personal data we retain and process (e.g. Spreadsheet, Database, Bespoke System etc).

6.1.4 Processing Conditions and Activities

At the core of all personal information processing activities undertaken by In-house Recruitment, is the assurance and verification that we are complying with Article 6 of the

GDPR and our lawfulness of processing obligations. Prior to carrying out any processing activity on personal information, we always identify and establish the legal basis for doing so and verify these with the regulations.

This legal basis is documented on our information audits and is also provided to the data subject and Supervisory Authority under our information disclosure obligations as outlined in this document. Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: -

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which we are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in In-house Recruitment
- Processing is necessary for the purposes of the legitimate interests pursued by In-house Recruitment or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).

As an organisation with less than 250 employees, In-house Recruitment maintains records of all processing activities and maintains such records in writing, in a clear and easy to read format and readily available to the Supervisory Authority upon request.

Acting in the capacity as a controller (or a representative), our internal records of the processing activities carried out under our responsibility, contain the following information: -

- Our full name and contact details and the name and contact details of the Data Protection Officer. Where applicable, we also record any joint controller and/or the controller's representative
- The purposes of the processing
- A description of the categories of data subjects and of the categories of personal data
- The categories of recipients to whom the personal data has or will be disclosed (including any recipients in third countries or international organisations)
- Where applicable, transfers of personal data to a third country or an international organisation (including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)
- Where possible, the envisaged time limits for erasure of the different categories of data
- A general description of the processing security measures as outlined in section 12 of this document (pursuant to Article 32(1) of the GDPR)
- Acting in the capacity as a processor (or a representative), our internal records of the categories of processing activities carried out on behalf of a controller, contain the following information: -
- The full name and contact details of the processor(s) and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer
- The categories of processing carried out on behalf of each controller

6.2 Where applicable, transfers of personal data to a third country or an international organisation (including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)

A general description of the processing security measures as outlined in section 13 of this document (pursuant to Article 32(1) of the GDPR)

CODES OF CONDUCT & CERTIFICATION MECHANISMS

[NOTE: At the time of writing this policy, neither the Supervisory Authority nor the European Data Protection Board have approved any Codes of Conduct or Certification Mechanisms pursuant to Articles 40-42 of the GDPR. Once such codes are published and authorised, if we follow such codes and/or become certified, we will detail such information in this section of the policy.]

In-house Recruitment adheres to the data protection codes of conduct prepared by [insert association/body] and/or are certified by [insert accrediting body] to demonstrate that we comply with the GDPR rules and principles. These codes and certification mechanism are approved by the Supervisory Authority and have been disseminated throughout the company to ensure competency and compliance from all staff.

T**he codes of conduct that we adhere to help us to: -**

- Improve transparency and accountability
- Demonstrate to the public and Supervisory Authority that we meet the requirements of the data protection law and that we can be trusted with personal data
- Mitigate against enforcement action(s)
- Improve standards by establishing best practice
- Carry out fair and transparent processing
- Ensure appropriate safeguards within the framework of personal data transfers to third countries or international organisations
- We submit to frequent and unscheduled monitoring and audits by the codes of conduct association/trade body and by the data protection certification scheme and understand that
- where we are deemed to be non-compliant in any area relating to the GDPR, we may lose our certification/seal of approval and/or the Supervisory Authority will be informed.

6.3 THIRD-PARTY PROCESSORS

In-house Recruitment utilise external processors for certain processing activities. We use information audits to identify, categorise and record all personal data that is processed outside of the company, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. Such external processing includes (but is not limited to): -

- IT Systems and Services: CHS Networks
- Payment Providers: PayPal, WorldPay, Pay360
- Platform Providers: Wordpress, Salesforce

We have strict due diligence procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain company documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

We audit their processes and activities prior to contract and during the contract period to ensure compliance

with the data protection regulations and review any codes of conduct that they are obligated under to confirm compliance. The continued protection of the rights of the data subjects is our priority when choosing a processor and we understand the importance of outsourcing processing activities as well as our continued obligations under the GDPR even when a process is handled by a third-party.

We draft bespoke Service Level Agreements (SLAs) and contracts with each processor and among other details, outlines: -

- The processors data protection obligations
- Our expectations, rights and obligations
- The processing duration, aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

That contract or other legal act shall stipulate, in particular, that the processor: -

- Processes the personal data only on our documented instructions
- Seeks our authorisation to transfer personal data to a third country or an international organisation

  (unless required to do so by a law to which the processor is subject)

- Shall inform us of any such legal requirement to transfer data before processing
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Takes all measures to security the personal data at all times
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights
- Assists In-house Recruitment in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments
- When requested, deletes or returns all personal data to In-house Recruitment after the end of the provision of services relating to processing, and deletes existing copies where possible
- Makes available to In-house Recruitment, all information necessary to demonstrate compliance with the obligations set out here and in the contract
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract
- Informs In-house Recruitment immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

6.4 RECORDS RETENTION & DISPOSAL

In-house Recruitment have defined procedures for adhering to the retention periods as set out by the relevant legislation and adhere to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as

confidential waste, secure electronic deletion) and priorities the protection of the personal data at all times.

Full details on our retention, storage and destruction policy and processes can be found in our Records Management Policy & Procedures and Secure Waste Disposal Policy. ICO in the Act. These procedures are found in our Records Retention Policy & Procedure document and the Retention Periods Register.

7.DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected at all times

whilst their data is being stored and processed by In-house Recruitment.

We therefore utilise several measures and tools to reduce risks and breaches for general processing, however when the processing is likely to be high risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where In-house Recruitment must or are considering carrying out processing that utilises new technologies, where there is a likelihood that such processing could result in a high risk to the rights

and freedoms of data subjects, we always carry out a Data Protection Impact Assessments (DPIA) (sometimes referred to as a Privacy Impact Assessment).

Pursuant to Article 35(3) and Recitals 84, 89-96, we consider processing that is likely to result in a high risk to include: -

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person(s)
- Processing on a large scale of special categories of data
- Processing on a large scale of personal data relating to criminal convictions and offences
- Systematic monitoring of a publicly accessible area on a large scale (i.e. CCTV)
- Where a processing operation is likely to result in a high risk to the rights and freedoms of an individual
- Those involving the use of new technologies
- New processing activities not previously used
- Processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects
- Processing activities making it difficult for the data subject(s) to exercise their rights

Carrying out PIAs enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach an allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

The PIA enables us to identify possible privacy solutions and mitigating actions to address the risks and protection the privacy and impact. Solutions and suggestions are set out in the PIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either: -

- Eliminated
- Reduced
- Accepted

7.1 DATA PROTECTION IMPACT ASSESSMENT PROCESS (DPIA)

A lead will always be appointed to carry out the DPIA, follow the process, record the necessary information and report the results to the Senior Management Team. All DPIAs are carried out in conjunction with the Data Protection Officer who provides advice and support for the compliance of the processes with the GDPR rules.

The DPIA lead ascertains if an assessment is required by assessing the answers to the below questions. Where one or more questions result in a 'yes' answer, the assessment is carried out.

Screening questions are: -

- Does the processing require systematic and/or extensive evaluation (via automated means) of personal aspects and individual(s)?
- Will decisions be based on such evaluations that are likely to produce legal effects concerning the individual(s)?
- Is the processing on a large scale and involves special categories of data?
- Is the processing on a large scale and involves data relating to criminal convictions and offences?
- Does the processing involve systematic monitoring of a publicly accessible area on a large scale? (i.e. CCTV)
- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Is the information about individuals likely to raise high risk privacy concerns or expectations?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information or a third-party without adequate safeguards in place?
- Does the processing involve the use of new technology or systems which might be perceived as being privacy intrusive?
- Could the processing result in decisions being made or action being taking against individual(s), in ways that could have a significant impact on them?
- Will the project require you to contact individuals in ways which they may find intrusive?

The PIA is carried out using our predefined document and each stage is recorded to demonstrate compliance and to show that all high-risk processing activities have been assessed prior to being operational. PIAs are retained for 6 years from the date they were first carried out and are readily available for the Supervisory Authority upon request. We will need to create a template in Word or Excel for completing our DPIA, using the below criteria.

The PIA includes: -

1. The aims and objectives of the DPIA
2. The scope of the DPIA (if covering more than one processing activity)
3. Clarify the legal basis for processing
4. Which activity/high risk reason is the DPIA required for (i.e. which of the initial screening questions above have been identified)
5. A description of the processing operations

6. The purpose(s) of the processing and where applicable, the legitimate interests pursued by the controller
7. An assessment of the necessity and proportionality of the processing in relation to the purpose
8. An assessment of the risks to individuals (including possible intrusions on privacy where appropriate)
9. Assess the corporate risks (including regulatory action, non-compliance, reputational damage, loss of public trust etc)
10. Conduct a compliance check against the GDPR, relevant legislation and any Codes of Conduct
11. Maintain a record of the identified risks
12. Where appropriate, we seek the views of data subject(s) or their representatives on the intended processing
13. The measures in place to address, reduce or remove the risk (i.e. security, proposed solutions, mitigating actions etc)
14. Data flow – what the information is, where it is coming from, who it is going to
15. Authorisation from the DPO and sign off by Senior Management
16. Record all PIA outcomes & add risk rating & next action

After the assessment questions have been addressed, internal and external consultations are held with employees, agents or third-parties who have a valid input of the processing activity to ensure that no risks go unmitigated. The Data Protection Officer and IT department are key contributors in the consultation stage, alongside colleagues who play an important part in the actual processing activity and/or protection of data.

The consultation can include: -

- Formal and informal discussions
- Emails and/or letters
- Employee, management & stakeholder meetings
- Board input and approval

After consultations, the processing activity is given a risk rating using the below 'Red, Amber, Green (RAG)' risk matrix. RAG rating is generated using the likelihood vs impact scores.

IMPACT					
	Trivial (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Almost Certain (5)	Low Med	Medium	High	Very High	Very High
Likely (4)	Low	Low Med	Med High	High	Very High
Possible (3)	Low	Low Med	Medium	Med High	High
Unlikely (2)	Low	Low Med	Low Med	Medium	Med High
Rare (1)	Low	Low	Low Med	Medium	Medium
Impact Score x Likelihood Score = Risk Rating					

- GREEN - Where an assessment outcome is Green, you/we should see if there are still any solutions or mitigating actions that can be applied to reduce the risk impact

down as far as possible. However, most green rated risks are acceptable and so focus should be placed on those with higher ratings. Even where a green RAG rating has been given at the risk/privacy identification stage, this risk should still be added to the mitigating actions template for continuity and to ensure that all risks have been recorded and assessed.

- AMBER - Where an assessment outcome is Amber, mitigating action must proposed and applied before processing can be approved. The aim is to reduce all risks down to a green (acceptable) level, however there will be occasions when processing must take place for legal/best interest reasons and so some processing with risks will go ahead and have to be accepted into the project. All solutions and mitigating actions must first be considered, tried and applied if possible.
- RED - Where an assessment outcome is Red, it indicates that either or both impact and/or likelihood scores are unacceptable and that complete solutions and mitigating actions would be required to bring both indicators down to an acceptable level. Some processing activities are eliminated at this point as the impact to individuals is considered to high risk to proceed.

However, in instances where the activity is essential or is a legal requirement, the proposed solutions and mitigating actions are applied and a further DPIA to see if the subsequent DPIA results in a Green and/or acceptable level of risk. If a high risk still exists and the processing activity is authorised, we will always consult the Supervisory Authority (SA) prior to processing and advise that the PIA indicates that the processing would result in a high risk and there is an absence of measures that can be taken mitigate the risk. You/we should then await written advice from the SA and provide all information requested by them during this period.

The above process enables us to devise ways to reduce or eliminate privacy risks and assess the costs and benefits of each approach, as well as looking at the impact on an individual's privacy and the effect on the processing activity outcomes. This enables us to document our identification and assessment of the risk, the solutions and mitigating actions used to reduce or eliminate the risk and records privacy risks which have been accepted as necessary for the project to continue.

LIKELIHOOD

The Supervisory Authority will in due course, pursuant to Article 35(4), make public a list of the kind of processing operations which are subject to a DPIA. Once published, you /we should add the areas on the list to this document.

8 DATA SUBJECT RIGHTS PROCEDURES

8.1 CONSENT & THE RIGHT TO BE INFORMED

The collection of personal and sometimes special category data is a fundamental part of the products/services offered by In-house Recruitment and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the GDPR.

The GDPR defines consent as; 'Any freely given, specific, informed and unambiguous indication of the data subject'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'.

Where processing is based on consent, In-house Recruitment have reviewed and revised all consent mechanisms to ensure that: -

- Consent requests are transparent, using plain language and is void of any

illegible terms, jargon or extensive legal terms

- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes
- Consent is always given by a statement or a clear affirmative action (positive opt-in) which signifies agreement to the processing of personal data
- Consent mechanisms are upfront, clear, granular (in fine detail) and easy to use and understand
- Pre-ticked opt-in boxes are never used
- Where consent is given as part of other matters (i.e. terms & conditions, agreements, contracts), we ensure that the consent is separate from the other matters and is not be a precondition of any service (unless necessary for that service)
- Along with our company name, we also provide details of any other third party who will use or rely on the consent
- Consent is always verifiable and we have controls in place to ensure that we can demonstrate consent in every case
- We keep detailed records of consent and can evidence at a minimum: –

    - that the individual has consented to the use and processing of their personal data that the individual has been advised of our company name and any third party using the data
    - what the individual was told at the time of consent how and when consent was obtained
    - We have ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including: -
    - Opt-out links in mailings or electronic communications
    - Opt-out process explanation and steps on website and in all written communications
    - Ability to opt-out verbally, in writing or by email
    - Consent withdrawal requests are processed immediately and without detriment
    - For special category data, the consent obtained is explicit (stated clearly and in detail, leaving no room for confusion or doubt) with the processing purpose(s) always being specified

8.1.1 CONSENT CONTROLS

In-house Recruitment maintain rigid records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent as it is to give consent.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorised by the Data Protection Officer prior to being circulated.

The GDPR states that where processing is based on consent and the personal data relates to a child who is below the age of 16 years, such processing is only carried out by In-house Recruitment where consent has been obtained by the holder of parental responsibility over the child. The UK's Data Protection Bill reduces this age to 13 years, as per Article 8(1) of the GDPR what advises that

"Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."

Consent to obtain, process, store and share (where applicable), is obtained by In-house Recruitment through: -

1. Face-to-Face
2. Telephone
3. In Writing
4. Email/SMS
5. Electronic (i.e. via website form)

Points 1-4 are enforced using scripts, checklists, on-screen prompts and signed customer agreements, to ensure that consent has been obtained and to remind employees of their additional consent obligations, as below.

Privacy Notices are used in all forms of consent to ensure that we are compliant in disclosing the information required in the GDPR in an easy to read and accessible format.

8.1.2 ALTERNATIVES TO CONSENT

In-house Recruitment recognise that there are six lawful bases for processing and that consent is not always the most appropriate options. We have reviewed all processing activities and only use consent as an option where they individual has a choice.

When reviewing the processing activity for compliance with the consent requirements, we ensure that none of the below are a factor: –

- Where we ask for consent, but would still process it even if it was not given (or withdrawn). If we would still process the data under an alternative lawful basis regardless of consent, we recognise it is not the correct lawful basis to use
- Where we ask for consent to process personal data as a precondition of a service we are offering, it is not given as an option and consent is not appropriate
- Where there is an imbalance in the relationship, i.e. with employees

8.1.3 INFORMATION PROVISIONS

Where consent is obtained; employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc) provide the below information in all instances, in the form of a consent/privacy notice: -

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of our data protection officer
- The purpose(s) of the processing for which the personal information is intended
- The legal basis for the processing
- Where the processing is based on point (f) of Article 6(1) "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party", details of the legitimate interests
- The recipients or categories of recipients of the personal data (if applicable)
- If applicable, the fact that In-house Recruitment intends to transfer the personal data to a third country or international organisation and the existence/absence of an adequacy decision by the Commission
- Where In-house Recruitment intends to transfer the personal data to a third country or international organisation without an adequate decision by the Commission, reference to the appropriate or suitable safeguards In-house Recruitment has put into place and the means by which to obtain a copy of them or where they have been made available

- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with the Supervisory Authority
- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- The existence of any automated decision-making, including profiling, as referred to in Article 22(1) and (4) and explanatory information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from the date of consent, unless there is a legal requirement to keep the information longer.

8.1.4 PRIVACY NOTICES

Where In-house Recruitment obtains personal data from a data subject or a third-party about the data subject, we utilise Privacy Notices to provide the information set out in section 9.1 of this policy and pursuant to Articles 13 and 14 of the GDPR. Our privacy notice is easily accessible, legible, jargon- free and inclusive of all information and is available in several formats as applicable to the method of data collection: -

- Via our website
- Linked to or written in full in the footer of emails
- In our Privacy Policy
- Worded in full in agreements, contracts, forms and other materials where data is collected in writing or face-to-face
- Verbally via telephone or face-to-face
- Via SMS
- Digital Products/Services

With lengthy content being provided in the privacy notice and with informed consent being based on its contents, we have tested, assessed and reviewed our privacy notice to ensure usability, effectiveness and understanding.

Privacy Notices are drafted by the Data Protection Officer using the GDPR requirements and with Supervisory Authority guidance

1. After a successful test, the acceptable Privacy Notice is rechecked against the GDPR and Supervisory Authority regulations and guidelines to ensure it still complies and is adequate and effective
2. The final Privacy Notice(s) are authorised by Senior Management/Director(s) before being rolled out

Where we rely on consent to obtain and process personal information, we ensure that it is: -

- Displayed clearly and prominently
- Asks individuals to positively opt-in
- Gives them sufficient information to make an informed choice

- Explains the different ways we will use their information
- Provides a clear and simple way for them to indicate they agree to different types of processing
- Includes a separate unticked opt-in box for direct marketing

8.2 PERSONAL DATA NOT OBTAINED FROM THE DATA SUBJECT

Where In-house Recruitment acts in its capacity as a data controller and where it has not obtained personal data directly from the data subject, In-house Recruitment ensures that the information noted in section 9.1.1 of this policy is provided to the data subject within 30 days of our obtaining the personal data.

In addition to the information that is provided to the data subject as set out in section 9.1.1, where the information has been obtained from a third-party, also advises the individual about: -

- The categories of personal data
- The source the personal data originated from and whether it came from publicly accessible sources

Where the personal data is to be used for communication with the data subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication or disclosure. Where In-house Recruitment intends to further process any personal data for a purpose other than that for which it was originally obtained, we communicate this intention to the data subject prior doing so and where applicable, process only with their consent.

Whilst we follow best practice in the provision of the information noted in section 9.1.1 of this policy, we reserve the right not to provide the data subject with the information if: -

- They already have it and we can evidence their prior receipt of the information
- The provision of such information proves impossible and/or would involve a disproportionate effort
- Obtaining or disclosure is expressly laid down by Union or Member State law to which is subject and which provides appropriate measures to protect the data subject's legitimate interest
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy

8.3 THE RIGHT OF ACCESS

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 (collectively, The Rights of Data Subjects), relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject’s identity (i.e. verbally, electronic).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request was received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional

circumstances and the data subject is kept informed in wiring throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: -

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- If the data has or will be disclosed to a third countries or international organisations and the appropriate safeguards pursuant to the transfer
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority Where personal data has not been collected In-house Recruitment. from the data subject, any available information as to the source and provider
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

8.4 DATA PORTABILITY

In-house Recruitment provides all personal information pertaining to the data subject, to them on request and in a format, that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

Where requested by a data subject for whom we hold consent to process and share their personal information and when processing is carried out by automated means, we will transmit the personal data directly from ourselves to a designated controller, where technically feasible.

To ensure that we can comply with Article 20 of the GDPR concerning data portability, we keep a machine- readable version of all personal information and utilise the below formats for compliance: -

- CSV
- HTML
- XML

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

8.5 RECTIFICATION & ERASURE

8.5.1 CORRECTING INACCURATE OR INCOMPLETE DATA

Pursuant to Article 5(d), all data held and processed by In-house Recruitment is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

Where we are notified on incomplete data, we will complete the information as directed by the data subject, including adding an addendum or supplementary statement where applicable. If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

8.5.2 THE RIGHT TO ERASURE

Also, known as 'The Right to be Forgotten', In-house Recruitment complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed. All personal data obtained and processed by In-house Recruitment is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

These measures enable us to comply with a data subjects right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

Where we receive a request to erase and/or remove personal information from a data subject, the below process is followed: -

1. The request is allocated to the Data Protection Officer and recorded on the Erasure Request Register
2. The DPO locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure: -
    1. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
    2. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
    3. the data subject objects to the processing and there are no overriding legitimate grounds for the processing
    4. the personal data has been unlawfully processed
    5. the personal data must be erased for compliance with a legal obligation
    6. the personal data has been collected in relation to the offer of information

society services to a child

7. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
8. The DPO writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure
9. Where In-house Recruitment has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. Such refusals to erase data include: -

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims

8.6 THE RIGHT TO RESTRICT PROCESSING

There are certain circumstances where In-house Recruitment restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subjects request.
Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit. Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

In-house Recruitment will apply restriction to data processing in the following circumstances: -

- Where an individual contests the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether we have legitimate grounds to override those of the individual
- When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure
- Where we no longer need the personal data but the data subject requires the data to establish, exercise or defend a legal claim

The Data Protection Officer reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third-parties. Where data is restricted and we have disclosed such data to a third-party, we will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the

restriction application and are also advised of any third-party to whom the data has been disclosed. We also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

8.7 OBJECTIONS AND AUTOMATED DECISION MAKING

Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material and provide an online objection form where processing is carried out online. Individuals have the right to object to: -

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- Direct marketing (including profiling)
- Processing for purposes of scientific/historical research and statistics

Where In-house Recruitment processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subjects' objection will only be considered where it is on 'grounds relating to their particular situation'. We reserve the right to continue processing such personal data where: -

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise or defence of legal claims

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, In-house Recruitment will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

We have carried out a system audit to identify automated decision-making processes that do not involve human intervention. We also assess new systems and technologies for this same component prior to implementation. In-house Recruitment understands that decisions absent of human interactions can be biased towards individuals and pursuant to Articles 9 and 22 of the GDPR, we aim to put measures into place to safeguard individuals where appropriate. Via our Privacy Notices, in our first communications with an individual and on our website, we advise individuals of their rights not to be subject to a decision when: -

- It is based on automated processing
- It produces a legal effect or a similarly significant effect on the individual
- In limited circumstances, In-house Recruitment will use automated decision-making processes within the guidelines of the regulations. Such instances include: -
- Where it is necessary for entering into or performance of a contract between us and the individual where it is authorised by law (e.g. fraud or tax evasion prevention)
- When based on explicit consent to do so
- Where the decision does not have a legal or similarly significant effect on someone

Where In-house Recruitment uses, automated decision-making processes, we always inform the individual and advise them of their rights. We also ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

9 OVERSIGHT PROCEDURES

9.1 SECURITY & BREACH MANAGEMENT

Alongside our 'Privacy by Design' approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our Information Security Policy & Procedures provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

We carry out information audits to ensure that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s). We have implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including: -

- Pseudonymisation and encryption of personal data
- Restricted access and biometric measures
- Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Disaster Recovery and Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Audit procedures and stress testing on a regularly basis to test, assess, review and evaluating the effectiveness of all measures and compliance with the data protection regulations and codes of conduct
- Frequent and rolling training programs for all staff in the GDPR, its principles and applying those regulations to each role, duty and the company as a whole
- Staff assessments and testing to ensure a high level of competency, knowledge and understanding of the data protection regulations and the measures we have in place to protect personal information
- Recheck processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal, it is rechecked and authorised by the Data Protection Officer

We have dedicated procedures for identifying, assessing and investigating compliance breaches and use a Breach Incident Form to record all information for consistency and compliance. Where a breach involves personal data, the Data Protection Officer will assist the Compliance Officer in the investigating and propose solutions and mitigating actions to prevent further breaches.

In the case of a personal data breach, we ensure that the Supervisory Authority is notified of the breach with immediate effect and at the latest, within 72 hours after having become aware of the breach. The Supervisory Authority is kept notified throughout the investigation and is provided with a full report, including outcomes and mitigating actions as soon as it is available. Where a breach is assessed by the DPO and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority.

However, breach incident procedures and an investigation is still carried out in full and the

outcomes and report are made available to the Supervisory Authority if requested. If for any reason, it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for the delay.

Where the breach has occurred with a processor appointed by In-house Recruitment our agreement outlines that they shall notify us without undue delay after becoming aware of a personal data breach.

The notification to the Supervisory Authority will contain: -

- A description of the nature of the personal data breach
- The categories and approximate number of data subjects affected
- The categories and approximate number of personal data records concerned
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (for obtaining further information)
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written format and in a clear and legible format. The notification shall include the nature of the personal data breach, the name and contact details of our Data Protection Officer, a description of the likely consequences of the breach and a description of the measures taken or proposed, to address the breach.

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational protection measures which render the data unintelligible to any person who is not authorised to access it (i.e. encryption, data masking etc) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

9.2 TRANSFERS & DATA SHARING

In-house Recruitment takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred. Data transfers within the UK and EU are deemed less of a risk than a third country or an international organisation, due to the GDPR covering the former and the strict regulations applicable to all EU Member States.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilise a process that ensures such data is encrypted with a secret key and where possible is also subject to our data minimisation methods. We use approved, secure methods of transfer and have dedicated points of contact with each Member State organisation with whom we deal. All data being transferred is noted on our information audit so that tracking is easily available and authorisation is accessible. The Data Protection Officer authorises all EU transfers and verifies the encryption and security methods and measures.

We conduct transfers of personal data to third countries or international organisations where

the Commission has advised that adequate levels of protections are in place. Such transfers are reviewed by the DPO and carried out following the same process as those within the EU. The DPO is responsible for monitoring the approved third country list provided by the Commission and only transferring data under this provision to those countries, organisations or sectors listed.

9.2.1 APPROPRIATE SAFEGUARDS

In the absence of a decision by the Commission on an adequate level of protection by a third country or an international organisation, we restrict transfers to those that are legally binding or essential for the provision of our business obligations or in the best interests of the data subject. In such instances, we develop and implement appropriate measures and safeguards to protect the data, during transfer and for the duration it is processed and/or stored with the third country or international organisation.

Such measures include ensuring that the rights of data subjects can be carried out and enforced and that effective legal remedies for data subjects are available. The appropriate safeguards can be provided without Supervisory Authority authorisation by: -

- A legally binding and enforceable instrument between public authorities or bodies
- Binding corporate rules
- Standard data protection clauses adopted by the Commission
- Standard data protection clauses adopted by a Supervisory Authority and approved by the Commission
- An approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights
- An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights

With authorisation from the Supervisory Authority, the appropriate safeguards may also be provided for by: -

- Contractual clauses between In-house Recruitment and the controller, processor or the recipient of the personal data in the third country or international organisation
- Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights

In-house Recruitment does not transfer personal data to any third country or international organisation without one or more of the above safeguards being in place or without the authorisation of the Supervisory Authority where applicable. We verify that any safeguards, adhere to the GDPR Principles, enforce the rights of the data subject and protect personal information in accordance with the Regulation.

Pursuant to Article 46, we ensure that any agreement, contract or binding corporate rules for transferring personal data to a third country or international organisation, are drafted in accordance

- with any Supervisory Authority and/or the Commission's specification for format and procedures (where applicable). As a minimum standard, we verify that the below are specified: -
- The structure and contact details of the group engaged in the activity and of each of its members
- The data transfers or set of transfers, including: -
- the categories of personal data

the type of processing and its purposes o
- the type of data subjects affected the identification of the third country or countries in question
- Their legally binding nature, both internally and externally
- The application of the general data protection principles, in particular: -
- purpose limitation
- data minimisation
- limited storage periods
- data quality
- data protection by design and by default
- legal basis for processing
- processing of special categories of personal data
- measures to ensure data security
- the requirements in respect of onward transfers to bodies not bound by the binding corporate rules

The rights of data subjects regarding processing and the means to exercise those rights, including the right: -

- not to be subject to decisions based solely on automated processing (inc. profiling) to lodge a complaint with the competent Supervisory Authority and before the competent courts of the Member States
- to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules

- Our acceptance (and that of any processor acting on our behalf) of liability for any breaches of the binding corporate rules by the third country or international organisation to whom the data is being transferred (with exemption from that liability, in whole or in part, only where we prove that we are not responsible for the event giving rise to the damage)
- How the information on the binding corporate rules and the information disclosures (Articles 13 & 14) is provided to the data subjects (with particular reference to the application of the GDPR Principles, the data subjects rights and breach liability)
- The tasks of any Data Protection Officer and/or person(s) in charge of monitoring compliance with the binding corporate rules, as well as monitoring training and complaint-handling
- The complaint procedures
- The mechanisms within the group engaged in the activity, for ensuring the verification of compliance with the binding corporate rules, including: -
- data protection audits methods for ensuring corrective actions to protect the rights of the data subject providing the Data Protection Officer and controlling board with such verification results
- The mechanisms for reporting and recording changes to the rules and reporting those changes to the Supervisory Authority
- The cooperation mechanism with the Supervisory Authority to ensure compliance by any member of the group, in particular by making available to the Supervisory Authority, the results of verifications of the measures referred to above
- The mechanisms for reporting to the competent Supervisory Authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules
- The appropriate data protection training to personnel having permanent or regular access to personal data

9.2.2 TRANSFER EXCEPTIONS

In-house Recruitment do not transfer any personal information to a third country or international organisation without an adequacy decision by the Commission or with Supervisory Authority authorisation and the appropriate safeguarding measures; unless one of the below conditions applies. The transfer is: -

- made with the explicit consent of the data subject, after having been informed of the possible risks and the absence of an adequacy decision and appropriate safeguards
- necessary for the performance of a contract between the data subject and In-house Recruitment or the implementation of pre-contractual measures taken at the data subject's request
- necessary for the conclusion or performance of a contract concluded in the interest of the data subject between In-house Recruitment and another natural or legal person
- necessary for important reasons of public interest
- necessary for the establishment, exercise or defence of legal claims
- necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register). Transfer made under this exception must not involve the entire personal data or categories of the personal data in the register and if the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

Where a transfer is not valid under Article 45 or 46 and none of the above derogations apply In-house Recruitment complies with the Article 49 provision that a transfer can still be affected to a third country or an international organisation where all the below conditions apply. The transfer: -

- cannot be made by a public authority in the exercise of its public powers
- is not repetitive
- concerns only a limited number of data subjects
- is necessary for the purposes of compelling legitimate interests pursued by In-house Recruitment which are not overridden by the interests or rights and freedoms of the data subject
- In-house Recruitment has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment, provided suitable safeguards with regard to the protection of personal data

[NOTE: The first three derogations are not available for the activities of public authorities in the exercise of their public powers.]

Where the above transfer must take place for legal and/or compelling legitimate reasons, the Supervisory Authority is notified of the transfer and the safeguards in place, prior to it taking place. The data subject in such instances is provided with all information disclosures pursuant to Articles 13 and 14, as well as being informed of the transfer, the compelling legitimate interests pursued and the safeguards utilised to affect the transfer.

9.3 PASSWORDS

Passwords are a key part of In-house Recruitment protection strategy and are used throughout the company to secure information and restrict access to systems. We use a multi-tiered approach which includes passwords at user, management, device, system and

levels to ensure a thorough and encompassing approach. Whilst passwords are also directly related to Information Security and Access Control, In-house Recruitment recognises to strong, effective and robust password controls and measures are imperative to the protection and security of personal information.

Passwords afford a high level of protection to resources and data and are mandatory requirements for all employees and/or third-parties who are responsible for one or more account, system or have access to any resource that requires a password.

9.3.1 PASSWORD CREATION & CHANGE

Only those authorised to access specific devices, information and systems are provided with the relevant passwords and such provisions are reviewed monthly to ensure that access is still valid and required. Employees may never share their passwords with anyone else in the company, including co-workers, managers or IT staff and unique passwords are used for all employees and access to systems and devices.

Employees are made aware that strong passwords are required for all systems and user-access and that a strict non-disclosure protocol applies to passwords. Where applicable to the system or device being used, In-house Recruitment utilises software to enforce the use of strong passwords.
Employees are not allowed to share or disclose any password.

Strong passwords are enforced on systems and by users and must be: -

- More than 8 characters
- Include letters, numbers and at least 1 special characters
- Not be easily recognisable (i.e. no names, dates of birth, places etc)
- Must include upper and lowercase letters

All passwords are changed monthly and users are not permitted to reuse the same password within a 3-month period. This is forced using software on all systems and a password change is automatically promoted at the start of each month. This change is enforced within 5 days of the change reminder being shown.

If a password is forgotten, only the IT Manager can reset the passwords. Passwords that have been forgotten are changed by default and cannot be reset to use the same password. A force change of password is also affected if the user suspects that the password has been compromised.

Where a password is reset, the individual's identity is first verified. This is essential where remote access passwords are changed or reset and the IT Manager is no able to physically verify the identity of the user. A two- step identification process is used in such instances with user-known variables being asked and answers verified prior to passwords being reset and disclosed.

9.3.2 DEFAULT PASSWORDS

It is occasionally necessary to set up default password at the IT Manager level. This is usually only when a new system or user are being set up and a password change will be promoted from the first user use. Default passwords are change as soon as is possible and where applicable, access to information is restricted until a strong password has been created. Where new systems, devices or software is purchased, default passwords are immediately changed and reset to use the strong variables indicated above.

9.3.3 PROTECTING PASSWORDS

In-house Recruitment is aware that viruses, software and phishing scams can attempt to obtain passwords at a user level. Whilst Firewalls are used to secure and protect systems and software, employees are provided with training and guidance on phishing and are instructed to neve disclose their passwords in a physical or online environment. This includes not disclosing passwords to third- parties, clients or representatives who may have a legitimate need to access a system.

Password fields are always displayed in a hash or star format (i.e. ### or ***) so that clear text is not present when a password is typed. This helps to prevent unauthorised access or password disclosure by copy & paste or electronic printing methods.

Writing down or storing passwords in any written or digital format is forbidden and all employees are made aware of this. Disclosure or unintentional loss of a password that has been written down in any format will result in disciplinary action being taken.

If a user fails to use the correct username and/or password when logging in to a system or device, we utilise generic failure messages that do not disclose the exact nature of the login error. After 3 failed attempts, the system will advise that login has failed, however it will not disclose if this is due to the username, password or both being incorrect. This aids in preventing brute force attacks or a non- authorised user being aware of which field is incorrect, which then increases their login attempts.

Where login fails, we operate a three-strike approach and the system will become unavailable for 15 minutes before the login can be re-tried. This protects against external 'bot' attacks and brute force.

10 AUDITS & MONITORING

This policy and procedure document details the extensive controls, measures and methods used by In-house Recruitment to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the GDPR and associated laws and codes of conduct. In addition to these, we also carry out regular audits and compliance monitoring processes that are detailed in our Compliance Monitoring & Audit Policy & Procedure, with a view to ensuring that the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The Data Protection Officer has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management Team where applicable. Data minimisation methods are frequently reviewed and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded by the Data Protection Officer and copies provided to Senior Management and are made readily available to the Supervisory Authority where requested.

The aim of internal data protection audits is to: -

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance
- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and actions plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data
- To monitor compliance with the GDPR and demonstrate best practice 11 TRAINING

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the GDPR requirements and its Principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role. Our Training & Development Policy & Procedures and Induction Policy detail how new and existing employees are trained, assessed and supported and include: -

- GDPR Workshops & Training Sessions
- Assessment Tests
- Coaching & Mentoring
- 1:1 Support Sessions
- Scripts and Reminder Aids
- Access to GDPR policies, procedures, checklists and supporting documents and Electronic Communications Regulations 2003, in respect to any related business activity.

We confirm that where individuals are concerned, we will only send direct marketing media (emails, calls or postal), when solicited (given direct prior consent) and will retain proof of all such consent for recording and auditing purposes.

Where any marketing material is delivered using an automated calling system, it will be done so only with the individual prior consent and any request to remove such consent will be recorded and applied with immediate effect.

We do not operate unsolicited tele-sales or marketing calls nor will any unsolicited sales or marketing attempts be made by fax.

11 PENALTIES

In-house Recruitment understands our obligations and responsibilities under the GDPR and Supervisory Authority and comprehend the severity of any breaches under the Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we breach the regulations, fail to mitigate the risks where possible and operate in a knowingly non- compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach. We recognise that: -

PRIVACY AND ELECTRONIC COMMUNICATIONS (PECR)

In-house Recruitment confirms that it complies with all regulations and laws made under the Privacy

11.1 Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

11.2 Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations (Chapter IX) or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

12 RESPONSIBILITIES

In-house Recruitment have appointed a Data Protection Officer whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection. The DPO will work in conjunction with the Compliance Officer, IT Manager and HR/Training Officer to ensure that all processes, systems and staff are operating compliantly and within the requirements of the GDPR and its principles.

The DPO has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the GDPR and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledge for the role they undertake.