Insignia Recruit Ltd
Insignia House, Unit 6, RO24 Harlow Business Park,
Greenway, Harlow, Essex CM19 5QB
0203 750 0575

Data Privacy Guidelines

These guidelines are issued in response to article 30 in relation to the protection of personal data.

Insignia Recruit Ltd aims to comply with all regulated guidelines and endeavours to protect the data of every person that is in contact with the company either as a candidate, client or employee.

Please see below the privacy guidelines and information on how we obtain, process, protect and delete the data that run through the company.

'The company' – means Insignia Recruit Ltd and any of its employees

'The client' – means every organisation and their employees that engages with the company in services and/ or products provided

'The candidate' – means every individual that comes into contact with Insignia Recruit Ltd and their employers with view of finding them their next career opportunity or to discuss their professional development

'Data Repository' – location of where the data is stored within the company. Data repositories are IT systems or physical locations of documents

Summary:

1. **Data Usage – What data is stored and how it is used?**
    a. **Candidate**
        i. **Document Types:** CVs, Photographic Documents (i.e. passport or driving licence), Proof of National Insurance Numbers (NI Card, payslips or HMRC document), Proof of address (i.e. Utility Bill, Phone Bill, Council Tax Letter or HMRC Letter), F002 Company Registration Form, F013 & F014 Job Offer Acceptance Form (Client / Candidate).
        ii. **Reason for processing:** These documents are requested and utilised for assisting the business and the candidates to secure employment and ensure their identity, proof of eligibility to work in the UK and confirmation of all the necessary information a client (i.e. employer company) will require to issue an employment contract and set up on their payroll.
        iii. **Storing said Data:** All data is retained for a max period of 5 years with the consent of the candidate. The data is stored in online file format only on a local server which is password protected and can only be accessed by employees using their individual log ins. All this data is backed-up on the company's one drive in the cloud which is also password protected and can only be accessed by authorised personnel using unique log ins and passwords. Some data may be found through our CRM (ClearBooks / Logic Melon) systems however these are also password protected to each individual employee that may require access to perform their duties for the company. No paper copies are stored, and any paper copies are scanned and saved in the online files before being shredded and disposed.
        iv. **Right to inspect and delete:** The candidate is aware they have the right to request copies of all data stored on them and have the right to request to have this data deleted regardless of time stored. The collection of data is done throughout the registration and job search process. During the registration the candidate has the option to opt in or out of the company storing their personal data. If they have opted out; this data will be deleted automatically after 60 days as this is a reasonable amount to of time between initially engaging our services and completing their job search. If they opt in, the data is stored for 5 years and then it is automatically deleted. If at any point, the candidate wishes to find out what data the company holds on them; it is all safely stored online in their personal files which we can then

supply all their information and permanently delete it at any point they request so. Any requests must be in writing via our enquiries@insignia-group.co.uk email address or an email address to one of our employees. All calls and emails will be deleted after 60 days unless they are saved within the candidates' online file which then will be according to their authorisation to retain the data for 5 years or not. At any point this data can be located and permanently deleted within the time frames specified for maximum time stored. This applies to all emails and phone calls as well.

b. Client

i. **Document Types:** This could be agreements, term of business, job descriptions, completed forms for processing of jobs and invoices.

ii. **Reason for processing:** This information is required for when the client engages the company to provide recruitment services. The data is stored in online file format only, on a local server which is password protected and can only be accessed by employees using their individual log ins. All this data is backed-up on the company's one drive in the cloud which is also password protected and can only be accessed by authorised personnel using unique log ins and passwords. Some data may be found through our CRM (ClearBooks / Logic Melon) systems however these are also password protected to each individual employee that may require access to perform their duties for the company. No paper copies are stored, and any paper copies are scanned and saved in the online files before being shredded and disposed.

iii. **Storing said Data:** Is stored in secure location online and via our CRM system.

iv. **Right to inspect and delete:** The client and their employees have rights to request what data is stored and can be deleted at their request. This data will be stored in the clients' online files or the CRM systems (LogicMelon / ClearBooks). We can easily identify these by searching based on the client's name. Once the working relationship ceases between the client and the company, all the data is stored for a max of 5 years in case of any queries. If an employee of the client leaves their organisation; their details are deleted from our system immediately; as long as the company is notified by the client in writing to enquiries@insignia-group.co.uk or notify an employee of the company. This applies to all emails and phone calls as well.

c. Employee

i. **Document Types:** This will be their CV, National Insurance, address, email, telephone number, next of kin, bank account details.

ii. **Reason for processing:** This is because the company needs to check for their eligibility to work in the UK, emergency contact details, payroll and for compliance.

iii. **Storing said data:** The company stores this online in a secure file where only the Business Directors, Owners or Approved Managers have access. All paper copies are stored in a locked filing cabinet by the Business Owners and Director's desk Michael Pagalos. The data is stored in online file format too, on a local server which is password protected and can only be accessed by the company's Directors using their individual log ins. All this data is backed-up on the company's one drive in the cloud which is also password protected and can only be accessed by the Directors using their unique log ins and passwords.

iv. **Right to inspect and delete:** The data is stored and can be inspected at the request of the employee at any time. The data is kept for a period of 10 years after the employee leaves the company for compliance, legal and offering references to potential future employer. It is stored under one central file with the employee's name and therefore easily locate all their data. We can delete all copies at their request including all emails and phone calls. Any requests must be sent to enquiries@insignia-group.co.uk or one of the Director's emails (vbarnes@insignia-group.co.uk or mpagalos@insignia-group.co.uk).

Insignia Recruit Ltd
Insignia House, Unit 6, RO24 Harlow Business Park,
Greenway, Harlow, Essex CM19 5QB
0203 750 0575

2. **Data Consent – How we obtain consent to store and use the data?**
    a. **Candidates:** We obtain their consent via the phone as prior to any candidate or applicant being submitted to a client would give us authorisation to. We also send them a candidate registration form to complete where we clearly state compliance with GDPR and the candidate has the option to accept or decline us retaining their information past the period required during their application process. Our calls are recorded, and the registration forms are saved in their files securely and online.
    b. **Clients:** We receive their information via email, call or through a meeting where they agree to work with us. The information is retained and as highlighted within this policy they have the same rights to know the information we hold on them and to delete as requested.
    c. **Employees:** We have held toolbox talks to discuss how they discuss GDPR with candidates and clients, however also how this affects their personal data stored within the company and re-iterated their rights as well. Toolbox talk has been held specifically relating to them, the contract terms and conditions have been amended for future new employees and a statement issued for existing employees to read, acknowledge and accept.
3. **GDPR – Transparency**
    a. GDPR is highlighted on candidate registration forms
    b. Displayed across our website
    c. Transparent through our employees
    d. Highlighted through our policy

4. **List of Data Repositories**

    There are 4 main data repositories:

    a. **Email System** – the company uses Office365 Exchange for all email communication. The system is providing data protection, breach, notification, role-based authentication and authorisation and data retention enforcement
    b. **Unstructured data** – the company is using on-premises internal shared drive. Shared drive provide encryption at rest of data, authorisation for data access based on log in credentials. All data are backed up to Office365 One Drive location where it is accessible by same level of authorisation as on on-premises shared drive
    c. **CRM Systems** – These are in the format of LogicMelon, ClearBooks or LinkedIn platform. All data is stored within this and can only be accessed via authorised personnel of the company with their unique individual log in credentials.
    d. **Call Recording system** – The company utilises RingCentral and record their calls. These are stored for a maximum of 60 days and then they are automatically deleted. Recordings can be accessed via the online platform which is secure and the company's employees can access their own recordings only with the use of their log in credentials.
5. **Data Retention Policy**
    a. The time frames involved in the retention of data is highlighted below:
        i. **Candidate data:** Held for 30 days if consent is not given while we process their application for a role and then permanently deleted. If consent is given to retain the data, we will retain it for a period of 5 years before automatically deleting it or gaining further consent.
        ii. **Client Data:** This is logged on our internal CRM until the contact leaves the client company or the client seizes to do business with the company.
        iii. **Employee Data:** This is retained for a max period of 10 years post the employee leaving the company. The reason for this is because we need certain information to confirm employment such as full name, dates of employment etc. The employee can request for non-relevant data to be deleted sooner of course.

Insignia Recruit Ltd
Insignia House, Unit 6, RO24 Harlow Business Park,
Greenway, Harlow, Essex CM19 5QB
0203 750 0575

6. **3rd Party Contracts**
    - **a.** We engage with a number of 3rd party providers who will give us candidate data, however they have received consent by the candidate for this data to be drawn upon by the company.
    - **b.** This will include CV databases, job board sites, external resourcing companies, LinkedIn etc
    - **c.** All data is used to contact the candidate, however after discussion if not of interest it is deleted straight away, or consent is gained by the candidate to retain their data.
    - **d.** Some examples of 3rd party contracts will be LogicMelon, Sourcebreaker, Totaljobs, LinkedIn, Indeed, Jobserve, Monster, ClearBooks etc.
7. **Staff Training**
    - a. All employees have undergone toolbox talks and Q&A sessions to ensure they comply with data privacy policy (copies of issued documents can be provided separately on request)
    - b. Also, the policy has been added to our internal induction process for any new employees who join the company and covered as part of our weekly team meetings.
8. **Data Protection Officer – Allocation of Responsibility**
    - **a.** The company is a small organisation so although we do not have an internal advisor / expert, the Business Director and Owner, Michael Pagalos has consulted various external consultants and used various material from memberships of the BIOR (British Institute of Recruiters) and FSB (Federation of Small Businesses) to shape the policy and ensure compliance.
9. **Enhanced Rights for Individuals – Subject Access, Right to be forgotten and Data Portability**
    - **a.** All individuals interacting with the company have the right to request all the information the company store on them and have the right to be forgotten and permanently deleted at any point; even if after they have given permission to retain their data.
10. **Data Breach Policy & Procedure**
    - **a.** The company endeavours for all their employees and systems to ensure the safety of the data we retain for business purposes.
    - **b.** In order to protect ourselves against possible breaches; all systems and files within the company are password protected and each employee and director have individual log ins and password. Access is granted in accordance to seniority and the requirements to have access to certain data for business purposes only.
    - **c.** In addition, notifications are sent to the Director instantly on any amends, changes, additions or downloads made on any of the files on our internal share drive or one drive. These are inspected, and any potential breaches reported and investigated.
    - **d.** If a breach is detected:
        - **i.** The Data Protection Officer will investigate the breach
        - **ii.** The individual(s) that the breach is in connection with, will be notified of the breach and all the follow up actions to ensure the security of their data
        - **iii.** An investigation into the breach will also be conducted and appropriate methods taken (e.g. training for employees, amendment of business processes or systems)
11. **Evidence of compliance actions taken**
    - **a.** A log is kept of all compliance checks / training / breaches or any other actions taken in relation to GDPR

Insignia Recruit Ltd
Insignia House, Unit 6, RO24 Harlow Business Park,
Greenway, Harlow, Essex CM19 5QB
0203 750 0575

1) Data Usage

Affected Category	Data Details	Examples	Data Repositories Used	Max Storage Time (Years)
Candidates (Any individual that is engaged with Insignia Recruit Ltd to find employment)	Name Address DOB ID Documents National Insurance No Employment History Salary Information Utility Bills	CV Passport NI Card Payslips Utility Bills Council Tax Letters HMRC Letters Internal Company Forms (F002, F013, F014)	**Internal Shared Drive** (We store all the documents in a password protected location with access permitted to only our internal staff, Business Consultants).	**5 Years** (From the date the data is first stored into the system)
Client (Any contact within any organisation that has consented and engaged in business with the company)	Client employee names, job title, contact details	Hiring Manager's name, email and telephone number	**Internal Shared Drive** (We store all information in a password protected location with access permitted to only our internal staff, Business Consultants). **CRM** (Their info is also logged against their company name in our CRM system)	**5 Years** (The data is deleted 5 years after the notice has been given by the client organisation to end the working relationship with the company. if the individual leaves the client organisation while the working relationship is in place then their data is deleted immediately regardless)
Employee (Any person employed directly by the company)	Name Address DOB ID Documents National Insurance No Employment History Salary Information Utility Bills	CV Passport NI Card Payslips Utility Bills Council Tax Letters HMRC Letters Next of kin Bank account details	**Internal Shared Drive** (We store all information in a password protected location with access permitted to only our internal staff, Business Consultants). **Directors Filing cabinet** (Paper copies are stored in the filing cabinet who only the Director / Owner Michael Pagalos has keys to. The cabinet is always kept locked and the key is with the director.	**10 Years** (The data and files are kept for 5 years after the employee leaves the organisation in case there are any follow up requirements and we need to consult their files. This could be in case a reference needs to be provided or any other information pertinent to a future application may be required).

Insignia Recruit Ltd
Insignia House, Unit 6, RO24 Harlow Business Park,
Greenway, Harlow, Essex CM19 5QB
0203 750 0575

Example of Compliance Log Sheet:

GDPR Compliance Log Book			
Date	**Description**	**Breach**	**Completed**
01/04/2018	GDPR Policy Finalised	N	Y
27/04/2018	GDPR Policy sent to external consultant for review	N	Y
01/05/2018	GDPR Policy issued to all employees	N	
01/05/2018	GDPR Letter issued to employees for their own data and saved in HR files	N	
04/05/2018	GDPR Training for employees	N	