ImaginativeHR

ImaginativeHR Privacy & Data Protection Policy

(Adjusted for General Data Protection Regulation (GDPR) (EU) 2016/679)

ImaginativeHR holds personal data about its prospects, clients, candidates, associates, partners and suppliers. ImaginativeHR takes its data protection obligations seriously and will only process personal information to:

- Connect to legitimate prospects, professional network contacts and partners in the broader commercial, Human Resources, learning and resourcing community;
- Administer our services to clients and partners in the UK, Europe and internationally;
- Provide services to individuals, teams and cross-organisation groups, (including e.g. candidates, coachees, mentees, assessment subjects and diagnostic subjects) who have specifically been referred to ImaginativeHR by our clients or partners, with a view to ImaginativeHR delivering services to them.

Effective 25th May 2018, European organisations are required to make changes in the ways that they process and hold personal data. The following Policy commitment contains revisions to our Data Protection Policy, in response to those changes:

1. **Personal data processing definition**: Processing personal data includes obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data. In the course of its activities, ImaginativeHR processes personal data as a necessary and legitimate requirement of its business and corporate social responsibility (CSR) interests.

2. **Data categories processed**: Personal data held by ImaginativeHR, under a range of circumstances, includes e.g.:

    - Names;
    - Photographs;
    - Job title;
    - Addresses;
    - Email addresses;
    - Telephone numbers;
    - Bank details;
    - Posts on social networking sites;
    - Qualifications;

ImaginativeHR: Company number: **08584916**
Call us on: ++44 (0)845 548 4321 / Email us on: info@imaginativehr.com / Web: www.imaginativehr.com
Registered office: The Old Wheel House, 31-37 Church Street, Reigate, Surrey, RH2 0AD, United Kingdom

- CVs and Bios (candidates, associates and partners);
- Testimonials (written and videoed);
- Survey responses;
- Salary (candidates only) and fees (associates only);
- Narrative project / assignment notes, including email records, relevant to each project / assignment, always recorded to a secure, password-protected, restricted-access database, following principles of brevity and confidentiality. (Whilst unusual; these notes may contain references to the families of candidates that we work with, including children, under 16 years of age).

3. **Lawful basis for processing personal data:** Lawful bases for processing information include 'Legitimate interests' and 'Consent'. In this regard:

   - *'Legitimate interests'* implies that the processing of personal data is necessary for ImaginativeHR's legitimate interests, unless there is a good reason to protect the individual's (data subject's) personal data, which overrides those legitimate interests. This is the basis of ImaginativeHR's processing of personal data in the majority of instances; save, in limited instances where it is determined that the data subject's rights may outweigh ImaginativeHR's legitimate interests;
   - *'Consent'* implies that the individual has given clear consent for ImaginativeHR to process their personal data for a specific purpose; where ImaginativeHR deems that such consent is appropriate.

4. **Data Controller and Data Processor definitions**: ImaginativeHR, as 'Data Controller' determines the purposes and means of collecting and processing personal data and is also responsible for processing personal data as 'Data Processor' under GDPR. ImaginativeHR is registered with the ICO (Information Commissioner's Office); with Data Protection Registration Number: **ZA011071**.

5. **Data subject rights**: Data subjects have the following rights, related to their personal data under GDPR:

   - Withdrawal of their consent, in writing, to the processing and holding of their personal data at any time. ImaginativeHR will have one month to respond to their request;
   - Refusal to consent to the processing of their personal data without any detriment to their treatment. ImaginativeHR will keep a list of data subjects who have asked for consent to be removed – this will be the only data that we will continue to keep;
   - The right to data portability, which means they have the right to transfer their data to another source or provider. This request must be in writing and ImaginativeHR is required to comply with requests within one month of receiving them;

- The right to make a Subject Access Request to their data. This means that they have the right to request verbally or in writing access to personal data held by ImaginativeHR about them. ImaginativeHR will generally have one month to respond to a request;

  (ImaginativeHR can refuse such requests, but must have a justifiable basis to do so. If ImaginativeHR refuses a request, it will advise the data subject regarding the reasons for refusal and will also advise that they both have the right to complain to the Information Commissioner's Office (ICO) and to a judicial remedy. ImaginativeHR will advise the individual about this without undue delay and at the latest within one month. ImaginativeHR can also charge for auctioning requests that are manifestly unfounded or excessive);

- The right to rectification of data;
- The right to erasure of data;
- The right to restrict processing of data;
- The right to be informed about arrangements for processing, handing and storing data.

6. **Data breaches**: Every care is taken by ImaginativeHR to protect personal data related to its prospects, clients, candidates, associates, partners and suppliers and to avoid any data protection breach.

   Data protection breaches could be caused by a number of factors; including e.g.:

   - Loss or theft of data and / or equipment on which data is stored;
   - Inappropriate access controls allowing unauthorised use;
   - Equipment failure;
   - Poor data destruction procedures;
   - Human error;
   - Cyber-attack;
   - Hacking.

   In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. In the case of a personal data breach, ImaginativeHR as the Data Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office (ICO). (Where the notification to ICO is not made within 72 hours, it shall be accompanied by reasons for the delay). The notification referred to above shall at least:

   - Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

- Communicate the name and contact details of ImaginativeHR's Data Protection Officer (this role shared by ImaginativeHR's Directors) or other contact point where more information can be obtained;

- Describe the likely consequences of the personal data breach;

- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

- Document the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with the Regulations.

In the event that the Data Controller identifies or is notified of a personal data breach; in addition to notifying the Information Commissioner's Office (ICO); the following correcting steps will be followed:

- The Data Controller will ascertain whether the breach is still occurring. If so, steps will be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant resources such as an IT technician;

- The Data Controller (or nominated representative) will also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, it may be necessary for ImaginativeHR to obtain legal advice;

- The Data Controller (or nominated representative) will quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

  - The use of back-ups to restore lost / damaged/stolen data;

  - If the data breach includes any entry codes or IT system passwords, then these will be changed immediately and the relevant agencies and members of staff informed;

  - Liaising with others to attempt to recover lost equipment;

  - Contacting relevant colleagues within ImaginativeHR, so that they are prepared for any potentially inappropriate enquiries (e.g. 'phishing');

  - If bank details have been lost / stolen, consider contacting banks directly for advice on preventing fraudulent use.

- In most cases, the Data Controller (or nominated representative) will fully investigate the breach. The data controller (or nominated representative) will ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation will consider:

  - The type of data;

  - Its sensitivity;

  - What protections were in place (e.g. encryption);

  - What has happened to the data;

- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (clients, suppliers. Etc.) and whether there are wider consequences to the breach.

- A clear record will be made of the nature of the breach and the actions taken to mitigate it. The investigation will be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office;
- A review of the causes of the breach and recommendations for future improvements will be concluded once the matter has been resolved;
- When notifying individuals, we will give specific and clear advice on what they can do to protect themselves and what ImaginativeHR is able to do to help them. We will also give them the opportunity to make a formal complaint if they wish. The notification will include a description of how and when the breach occurred and what data was involved. We will include details of what we have already done to mitigate the risks posed by the breach;
- Once the initial aftermath of the breach is over, the Data Controller (or nominated representative) will fully review both the causes of the breach and the effectiveness of the response to it. If systemic or ongoing problems are identified, then an action plan will be drawn up to put these right and mitigate against breaches like this happening again. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

7. **Data audits**: From time to time, ImaginativeHR will audit the personal information held, where it came from and who we share it with. We will also maintain records of our processing activities in this policy. This complies with the GDPR's accountability principles.

8. **Data storage**:

- Data will normally be stored for up to 6 years after the last active contact. After this period personal data will be removed or destroyed;
- Save for any initial notes taken during meetings or calls with data subjects or assessment / email records / survey / mailer data which is captured via / to third-party platforms; all ImaginativeHR data is captured to ImaginativeHR's database and its corresponding Mobile Application (App), which is secured via multi-level authentication and open to limited access by a limited number of ImaginativeHR data processors;
- Any emails sent over unencrypted systems are relatively unsecured and ImaginativeHR provided the following disclaimer in its email communications:

> *This email and any attachment are sent in confidence and upon the basis that the recipient will conduct appropriate virus checks. If you receive this email in error, please telephone ImaginativeHR on ++44 (0)845 548 4321 or contact us here upon receipt. You are strictly prohibited from using; copying or disseminating this email or any information contained in it, save to the intended recipient. Internet*

communications are not secure and ImaginativeHR is not responsible for their abuse by third parties, nor for any damage or loss caused by any virus or other defect.

- Access to ImaginativeHR systems by anyone other than ImaginativeHR employees for maintenance or other reasons will be done with adequate supervision. The amount of supervision will depend on the potential for access to data by the external person and whether they are on or off site.

9. **Security and privacy technologies**:

- All ImaginativeHR computers employ an industry-standard software firewall and have industry-standard anti-malware software installed. Malware definitions are updated at least daily;
- All incoming and outgoing data is scanned for viruses, as will any disk or CD that is used;
- A full system scan is regularly completed on each machine;
- Incoming and outgoing emails are scanned for malware and other malicious content and mails are quarantined as necessary.
- All business critical software including operating systems are kept up to date with security patches and service packs.

10. **Data protection awareness and training**:

- All ImaginativeHR employees, associates and partners are made aware of ImaginativeHR's Data Protection Officer and their role within the organisation and will be kept informed as to the identity of the person to whom such notifications should be made;
- ImaginativeHR employees know where to find details of the information security standards and procedures relevant to their role and responsibilities;
- ImaginativeHR employees are trained about the common methods that can be used to compromise our systems;
- ImaginativeHR employees are trained to understand and recognise the signs of a Security Incident – any event that can damage or compromise the confidentiality, integrity or availability of ImaginativeHR's business–critical information or systems. This will include: strange phone requests, especially for information; unusual visitors; strange patterns of computer activity; unusual appearance of computer screens; and computers taking longer than usual to perform routine tasks.

11. **Incident response management and business continuity**:

- ImaginativeHR enforces monthly database backups, including all database records. The company holds the past 3 months' backup records at any time.

- ImaginativeHR maintains an up-to-date Disaster Recovery Plan to ensure business continuity in the event of a serious Security Incident. The plan specifies:

  - the designated people involved in the response; external contacts, including law enforcement, fire and possibly technical experts;
  - contingencies for foreseeable incidents such as: power loss; natural disasters and serious accidents; data compromise; no access to premises; loss of essential employees; and equipment failure.

- ImaginativeHR ensures that its Disaster Recovery Plan is tested at least once a year, regardless of whether there has been a Security Incident.

- The Disaster Recovery Plan is re-examined and updated after every incident and after every test, as necessary, using the lessons learned.

Where data subjects are not satisfied with ImaginativeHR's response or believe we are processing personal data in breach of current regulations, they are entitled to complain to the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113.