Data Protection Corporate Policy

Version: 03

Date: 04 July 2019

Contents

PIR INTERNATIONAL
Search & Interim For Life Sciences

Purpose

The purpose of this policy to show PIR's compliance with the General Data Protection Regulation (GDPR) guidance which were implemented by the UK Government in May 2018 under The Data Protection Act (DPA) and new European regulations.

The Data Protection Act 1998

Companies processing personal data are required to abide by the eight principles of the Data Protection Act 1998 ("DPA"), which require that data is:

1. Personal data shall be processed **fairly and lawfully** in particular; it shall not be processed unless:
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more **specified and lawful purposes** and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be **adequate, relevant and not excessive** in relation to the purpose or purposes for which they are processed.
4. Personal data shall be **accurate** and, where necessary, updated.
5. Personal data processed for any purpose(s) shall **not be kept for longer than is necessary** for that purpose or those purposes.
6. Personal data shall be **processed in accordance with the rights of data subjects** under this Act.
7. Appropriate **technical and organisational measures shall be taken against unauthorised or unlawful processing** of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall **not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection** for the rights and freedoms of data subjects in relation to the processing of personal data.

Personal Data (PD) means data, which relates to a living individual who can be identified from the data or from the data together with other information, which is in the possession of, or is likely to come into possession of PIR. Data may only be processed with the consent of the person whose data is held. The definition of "processed" is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes both hard copy and electronic data.

Objective

The objective of this policy is to ensure that all external stakeholders and PIR employees are aware of PIR's policy regarding the processing of PD, and that employees are fully aware of the requirements and obligations required of them and PIR under DPA.

The policy will show the steps that PIR have taken to clean/check PD held in the Customer Relationship Management (CRM) database (hereafter called the database), supplier and employee records, in both hard copy and electronic format.

The policy will also describe the processes which is followed by PIR to ensure ongoing compliance with the DPA including employee training.

Policy Statement
PIR is committed to ensuring that all PD is processed in line with the DPA. To comply with the principles of the DPA, as outlined above, personal information will be collected and used fairly, stored safely and not disclosed to any other person or organisation unlawfully.

PIR is required to keep certain information regarding its employees to enable it to carry out its day to day operations, and to comply with its legal obligations. GDPR guidelines have also been applied to this data.

Responsibilities
PIR is registered with the Information Commissioners Office (ICO) and has appointed a Data Controller Jayne Fergusson jayne@pir-intl.com 01480 499580 who is responsible for ensuring the provision of suitable DPA advisory, training and awareness, DPA request handling, and compliance with the PIR's obligations under the DPA.

It is the responsibility of all employees to ensure that they understand their obligations under the DPA, and to inform the Data Controller if they do not; and all data processed is done so in line with this policy.

All data subjects have the right to access the information held about them, ensure that it is accurate and fairly held, and to inform the Data Controller if they are dissatisfied. All requests to access PD will be handled in accordance with the DPA. Data subjects include all employees and any other person about whom PIR processes PD.

PIR may not always seek the consent of data subjects when processing PD, for example, when processing for legitimate business purposes or when the information is available in the public domain. Contacts are populated via business contacts, networking and referrals. This information is only used for legitimate business purposes. Contacts can unsubscribe from being contacted at any point; however, their record would not be removed to prevent them subsequently being re-added to the database.

Everyone who provides PD to PIR is responsible for ensuring adherence to the DPA, especially with regard to accuracy and, in the case of third parties providing the PD of others, the right to disclose this data.

Procedure

Preparation for GDPR
PIR undertook to clean the database, server and hard copy filing/files prior to implementing the new GDPR guidelines and internal processes in 2018. The following actions were taken:

- **Legitimate Access Form:** The legitimate access form was completed by BOD on behalf of PIR
- **Database**: For candidates the following attempts were made to make contact:

1. Records which had not been active or were incomplete with no contact details (email or telephone number) were removed.
2. Where no email but a phone contact was available, at least one attempt was made to contact the person to see if they wished to update their record or have it removed. If possible, a voicemail was left. If the number was disconnected or unobtainable and there was no business reason to retain the record it was deleted.
3. Following the above steps, a generic email was sent to all candidates informing them their data was being kept by PIR and would only be removed if they requested PIR to do so. If an email was undeliverable the candidate was assessed by the team and if it was felt relevant to the business to retain the record was followed up by a phone call. If there was no business reason to retain the record it was deleted.

- **Server**: Under the PIR 'Executive Search' process prospective candidates PD is recorded on a spreadsheet during the initial client project. As this data is classed as business critical for a period of time following the closure of the 'Executive Search' it has been agreed that from the job closure date (Job closure = the date the role is filled by PIR or cancelled by the client) the spreadsheet would be kept for 5 years. After the first year the personal contact details (email/ phone numbers) of both the prospective and registered candidate contacts would be deleted from the spreadsheet leaving only their names, occupations and place of work. Each spreadsheet will be totally deleted 5 years post the job closure. Any PD for registered candidates will have been stored on the database which is held in the cloud and backed up on the database supplier. All other PD records (i.e. candidate reports, notes) stored on the central server have been deleted as these are stored on the database.
- **Employee records**: All electronic and hard copy PD was cleansed by the then BOD. Hard copy data which needs to be retained for legitimate business purposes is stored in a secure cabinet. Any electronic PD has been moved to a secure folder within the PIR server which is only accessible by the CEO, Sally Hope, Founder & NED, Carolyn Douthwaite, Projects Director Jayne Fergusson, IT provider and accountant, as applicable.
- **Interim contractors**: PIR is required to keep certain records for candidates on interim contracts with PIR. Due diligence documents are stored on the database and contracts containing home address details are stored on the database or on the PIR server.
- **Suppliers**: All suppliers were asked to provide information on their GDPR process, preparation and policy. All responses with any accompanying documents have been filed in the relevant GDPR file / folder.

Personal Data Processing

As a recruitment agency PIR needs to collect, store and disseminate PD on their candidates in order for the business to function. Data is received / retrieved in various ways and formats. PIR aim to process all data in line with GDPR.

Informing

When receiving new or updates to candidate's PD, PIR employees will inform the candidate either verbally or in writing that their data will be kept on our electronic database. They will also be informed (verbally or via link to PIR's Privacy Policy):

- Their personal data will be stored securely on our database
- PIR will never share their data with any external marketing source
- Their permission will be sought before their data is shared with any client with regards to opportunities
- Further information on PIR's Privacy policy can be found on the PIR website
- They can ask for their PD to be updated or removed at any time

Any information on candidates not received directly through them will not be stored on the database without their permission. Candidates contacted through other means / sources i.e. LinkedIn will not be stored on the database without the candidate's permission.

Candidates rights:

GDPR talks of the right to have data portability allowing individuals to obtain and reuse their PD for their own purposes across different services. PIR will share copies of PD via the subject access request procedure through the CRM system who will then allow access to an online portal.

Request for data review:

Anyone may request to review their PD held by PIR at any time. The request must be sent in writing (via email). Once the request is received by PIR a check will be made that the request comes from a legitimate source, if necessary, a member of the PIR team may call them to confirm the request. If confirmed as a valid request the data will be supplied within 5 working days assuming the CRM provider can give access this quickly. Any data supplied will be done so online and will be password protected. The request will be logged onto a 'GDPR Requests' spreadsheet under the candidate tab held on PIRs server as there is no tracking reports on the CRM.

Request for data correction:

If a person believes their data is inaccurate, they need to send a request stating what data needs to be amended / updated to the Data Controller. Once this has been received by PIR the request will be assessed, if there is no valid reason for the data not to be corrected this will be done within 5 working days wherever possible and the new data subject access request sent via the CRM with a request for confirmation that their data is now accurate.

If there is a valid business reason why the data should not be amended / updated the Data Controller will inform the person explaining the reason and offer the opportunity for the record to be deleted. As PIR do not own the database or have any ability to edit certain datasets there maybe occasions where data cannot be edited but new data or notes can be added. The CRM have introduced the ability to update journal entries so inaccurate data should be able to be rectified.

Request for data deletion (right to erasure / right to be forgotten):

Anyone has the right to request for their data to be removed from the database at any time. The request needs to be in writing and will be processed by the Data Controller. Once the data has been deleted the Data Controller will inform the requestor that this has been completed. If there are business reasons why part or all of the data cannot be removed due for a legitimate business purpose PIR will delete the record and add a shell record to enable the business to retain the information, it legitimately needs. These shell replacement records will be tracked on the GDPR Requests spreadsheet.

A shell record will contain the minimum amount of information required by the business this will include name and general functional focus along with a note as to why PIR should not approach this person. This will prevent the person being approached by the team via networking / social media or being re-added at a subsequent date. The CRM does allow restriction of records to leaving only the ID and name of the person, but this does not allow PIR to review why the person was restricted and leaves PIR at risk of lifting the restriction to review the information, allowing full access to data that was requested to be removed.

Data Storage

All PIR IT equipment is password protected and backed up internally by our supplier (for supplier information see suppliers). Each employee has their own username and password for computers, mobile phones and the database, these passwords should not be shared with other employees. A master sheet of all passwords is kept by Ilux our IT consultants.

Candidate and Client data is mainly stored on the database which is accessed via our own server. Data stored on the database is only accessible to PIR employees and the database supplier (for supplier information see suppliers). At times PIR may use external researchers, they will not be given access to the database.

For 'Executive Search' roles prospective candidate data is initially put onto a project spreadsheet (Excel), this data is usually retrieved from the public domain i.e. LinkedIn or networking/referrals. Once a candidate has registered (consented for PIR to store their PD) their information will be added to the database, with their permission. When a 'Executive Search' role has been closed the data on the spreadsheet will be kept for business-critical purposes for 5 years following the closure of the 'Executive Search' and then deleted.

If PIR experience any security breach they will make every endeavour to inform candidates asap of the nature of the breach and what information has been lost. As PIR only holds limited amount of 'high risk' data i.e. financial data any high security breach is only likely to affect a small number of candidates. PIR are reliant on our supplier's processes and procedures on how / when we are informed of any potential data breach (for all supplier information see suppliers). If a member of the PIR team discover a data breach they will immediately notify Sally Hope, CEO and the relevant supplier(s). If the breach is likely to result in a high risk of affecting any individual's data privacy the individual will be informed of a potential identity theft.

A notifiable breach must be reported to the relevant supervisory authority (ICO) within 72 hours of the organisation (PIR) becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows for information to be provided in phases. Failure to notify the authorities of a breach can result in a significant fine.

Business Usage:

As a recruitment agency PIR needs to collect, store and disseminate PD on their candidates and contacts, in order for the business to function. Recipients can 'unsubscribe' to any PIR mailers at any time. PIR never sells or shares data with other agencies / organisations.

Talent Mapping:

Talent Mapping is a service that PIR provides to clients for pipelining for future gaps or benchmarking. Talent Mapping varies from company to company depending on the specific level / role they are looking to map. The information provided is 'real-time', which has been extracted from public domain and would only consist of: name, job title and company name.

Talent Mapping is often a first step in the search process prior to PIR anonymously approaching contacts directly on behalf of the client and finding out about the contacts background, potential for a move etc. In line with GDPR, if the client requests this level of details the contact would be informed that PIR were performing a talent mapping / pipelining and consent would be gained before sharing further information with the client which will no longer allow this to be an anonymous process.

Any Talent Mapping document (Word / Excel) will be handled under the same process as the 'Executive Search' spreadsheets.

Transferring data to clients:

With the nature of PIR's business some candidate data will be transferred to the client to enable us to provide the client with the recruitment service we are fulfilling. Before any PD is transferred permission will be obtained from the candidate. Once the data has been transferred to the client it is the client's responsibility to ensure the data is held / stored securely. Their employees are also bound to adhere to their internal policy on Data Protection. PIR makes every effort to highlight GDPR responsibilities.

The following statement appears on any document (i.e. CV or Candidate Report) which contains candidate data and is sent to the Client.

> The data enclosed in this document is confidential and must to be controlled / shared in line with your GDPR / Data Protection guidelines. PIR expect all information to be destroyed when appropriate and no additional copies saved or stored, as defined in our Privacy Policy which is available to review on our website.

A reminder will be included in the email containing PD that the data is Confidential and must be stored under GDPR guidelines and in line with PIR's client / supplier contract.

Due Diligence (DD) / Candidate References:

References and DD needs to be performed if a candidate is offered a role. PIR are under a legal obligation to collect and process this data. The amount of information needed is dependent on if the role is **Interim** or **Executive Search**.

Executive Search:

- CV
- Passport (proof of eligibility to work in UK)
- References

Interim:

- CV
- Passport (proof of eligibility to work in UK)
- References
- Limited Company documents:
    - Certificate of Incorporation
    - Professional Indemnity Insurance
    - VAT certificate

When taking up references for candidates the minimum amount of personal referee information will be recorded in the database. The name / role / company of the referee will be retained for DD compliance.

Copies of the other documents required to confirm DD and eligibility to work in the UK will be uploaded to the database and stored. This information will not be stored outside the database and will be deleted from emails etc.

Suppliers:

All PIR suppliers have been informed that PIR require that they work to the strictest data protection policy. They have also been asked to provide PIR with information on their GDPR policy.

Information received from the suppliers has been checked by the Data Controller for compliance and filed in the GDPR folder for referencing. All suppliers have been advised of PIRs expectations re: data access, confidentiality and data processing.

Shredding company

A secure shredding waste bin is provided at the PIR premises. The bin is emptied once a month and shredded off site. A certificate is provided to confirm the bin has being collected and a destruction certificate to show the bin contents have been destroyed securely and in line with the supplier's policies. These certificates are filed in the supplier folder.

Answer phone service

This service provides an out of office answering service by actual people who can transfer calls to PIR employees or email messages to the appropriate person.

Cleaners

A clear desk policy is in place to minimise the risk to PD potentially being left out. The cleaning service has no legitimate access to any PIR IT systems / equipment and all laptops / paper records (inc. CVs, notes / notebooks) should be locked away in desk drawers at night.

I.T. Services

Our I.T. provider adheres to their own policy for dealing with server security, back-up and breaches. A copy of this is on file in the GDPR folder.

Our provider never removes any data from the PIR servers, unless explicitly instructed to do so in writing. As system administrators they don't automatically have rights to access data but need to request authorisation from PIR. Their staff are Disclosure and Barring Service (DBS) checked where applicable and systems are encrypted where possible. Passwords, backups and system information is stored in encrypted databases and all information is encrypted before leaving the client site.

General IT system information:

- All data is backed daily and retained for 30 days per backup
- Data is backed up on our server and at an Ilux data centre
- All deleted emails removed from the personal deleted folder are purged from the system
- All PIR computers are password protected and secured in a locked office if they are not off site
- An automatic anti-virus program is installed on all computers and a scan is run on a daily basis

For I.T equipment security please see section on 'Training'.

Web provider

PIR's website is hosted externally and is backed up on secure services in a robust manner. Information about the hosting and back up services can be found in the supplier's contract / proposal. There is no PD held on the website. If a mailing list is to be created this would be done via a third party such as Mailchimp and data held securely in their back end.

Accountant / Bookkeeper

As PIR's accountants and bookkeeper, their employees have access to PD for all PIR employees and interim placements as PIR have a legal obligation to report information to the HM Revenue & Customs (HMRC) which includes PD. They do not have access to the database but manage and maintain the financial systems on the Sage accounting software. The Sage software is only stored on relevant PIR computers and is only accessible by the CEO, Projects Director, Bookkeeper and Accountants. All Sage files are stored in the secure area of the PIR server.

All paper financial records are stored in a secure cabinet which is locked. Keys are held by Jayne Fergusson Projects Director, and Sally Hope, CEO.

CRM database

Our database provider adheres to their own policies for dealing with the database security, back-up and breaches. A copy of this is on file in the GDPR folder.

The database holds all candidate / client records, this is only accessible via an internet portal which has individual password protection for each employee. The database is backed up on the providers servers.

Photocopier

Note: EasyCopier informed us that all printing and scanned data is stored in printers and printer will need to be wiped when it is returned to supplier (at a cost to PIR). See letter: R:\#3- Operations\Processes\GDPR\PIR Suppliers\EasyCopier-GDPR Aware Notice-Sep 18.pdf

Employee data

All employee / ex-employee documents whether in paper or electronic format are stored in a secured cabinet / IT folder. The data is only accessible by, Sally Hope, CEO and Jayne Fergusson Projects Director has access to H&S, Induction, and support information. Employee PD is sent to the Payroll, Healthcare and Pension providers as necessary to enable various benefits and business processes to be carried out.

Under current UK laws employee / ex-employee data needs to be kept for a defined period. Once this period has passed and, there is no business reason to retain the information for a longer period individual's data will be deleted / destroyed as applicable.

When conducting internal recruitment PIR retain PD on potential candidates which may have been provided by a recruitment agency or an individual candidate. These records will be kept throughout the recruitment process and destroyed securely at the end. When a candidate is appointed to a PIR post their PD will be treated as per the employee processes.

Retention Timelines for employee documents (as advised by our employment law specialist):

- **Application Form:** Duration of employment plus 6 months
- **References Received:** Duration of employment plus 6 months
- **Payroll and Tax Information:** 3 years from end of year they are related to
- **Sickness records:** Duration of employment plus 6 months
- **Recruitment Information:** Duration of employment plus 6 months
- **DBS Disclosures:** Duration of employment plus 6 months
- **Probation Information:** Duration of employment plus 6 months
- **Health Information:** as required
- **Annual Leave Records:** Duration of employment plus 6 months
- Unpaid Leave / Special Leave Records: Duration of employment plus 6 months
- **Parental Leave:** 6 years
- **Supervision Records:** 3 years
- **Annual Appraisal / Assessment Records**: Duration of employment plus 6 months
- **Records Relating to Promotion, Transfer, Training, Disciplinary Matters:** Duration of employment plus 6 months
- **References Given / Information to Enable References to be Provided:** 6 years from reference / end of employment
- **Summary of Record of Service e.g. name, position held, dates of employment:** 6 years from end of employment
- **Records Relating to an Accident of Injury at Work:** 6 years

Current employee data

In order to process current employee's remunerations and benefits some PD is shared with the following suppliers:

- Pensions
- Healthcare
- Payroll / Accountants

All employees are aware that PIR shares their data with these companies and for healthcare and childcare vouchers this is an opt in scheme for which employees receive information directly from the individual companies.

The pension scheme has an opt out process, but all employees must be registered on the pension system which is accessed via a secure internet portal. The PIR employer password login is held in a secure protected file on the PIR server. All employee and ex-employee's information must be stored on this system under PIR's legal obligations. PIR use the online system which is provided by our pension supplier.

Training

PIR employees will be trained on the DPA / GDPR best practice as part of their induction. PIR will hold an annual refresher on DPA. Employees will all sign a training record for training received which will be kept in their personnel files. The employees understand that any disregard of the processes and policies can result in disciplinary action.

IT Equipment

PIR provides all staff with IT equipment (laptop and mobile devices) which should be used for business purposes. No PIR information / data should be stored on any personal IT equipment.

If IT equipment is taken off-site PIR expect standard precautions to be taken to ensure the equipment is safe / secure:

- Securely stored
- Don't leave on seat of car / in plain sight
- Don't leave unlocked in public places
- Don't leave unattended

If any IT equipment is lost or stolen this should be reported as soon as possible to Jayne Fergusson, Projects Director or Sally Hope, CEO in line with the PIR Phone/Laptop policies. IT/Database suppliers should be notified immediately to arrange for access/passwords to be stopped/changed to limit damage to any system.

Best Practice

All employees are encouraged to implement best practice for keeping as little additional/temporary information (emails, paperwork including any notes / post-it notes) as possible on laptops, desks and within outlook. When candidate consent is in place this information should be stored on the database and should not be retained in other formats once the role has been closed. All paperwork will be place in the shredding bin for secure disposal.

Compliance

PIR will review this policy on a regular basis to ensure its relevance and effectiveness.

Any queries regarding this policy should be raised in the first instance with the Data Controller, Jayne Fergusson jayne@pir-intl.com / 01480 499580 or 07725 041754.

Reference Documents

- The Data Protection Act https://www.gov.uk/data-protection
- PIR Documents:
    - Privacy Policy
    - Employee Contract
    - Employee Handbook
    - Operations Manual
    - Terms of Business (TOBs)
- Electronic GDPR folder PIR/GDPR
    - GDPR Policy
    - Training-Crib Sheets Docs (Folder)
        - Training slides
        - Crib sheets - GDPR and Consent Flow on BOND
        - Training sign off
    - Client Information (Folder
        - Client Candidate Privacy Policies
        - Emails from Clients
    - GDPR-Search Due Diligence Spreadsheet
    - GDPR-Requests Spreadsheet
    - GDPR-Client Candidate Privacy Policies/Interactions Spreadsheet