GDPR Policy

Ver 1:0

Date 17th May 2023

This policy is compiled from the GDPR Directives outline in our ISO 27001:2013 Aspects Policies and a second Policy document designed to Change Spinwell's Lawful Basis from Consent to Legitimate Use

GDPR – Change of Lawful Basis from Consent to Legitimate Use

Version 1:0

24th March 2022

Since moving our CRM from EBoss to EPloy, we have been regularly reaching out to the candidates on our database in order to get their consent to remain active upon it. The settings have meant that if candidates did not respond within a set time frame they would receive a reminder email. This has led to acrimony as some have received up to 12 reminders. The latest attempt to get consent from existing candidates on our database has led us to believe that we can expect to lose about 75% of all those kept on there. This could be untenable for the business, therefore we tried to identify a different method of maintaining our database. Information from APSCo and ICO has led us to believe that most of our competition operate on a "legitimate use" basis as opposed to a "consent" model based on the information below:-

"Processing is lawful if it is necessary for the purposes of the legitimate interest pursued by the controller (you) or a third party except where protecting the interests and rights of the data subject are more important, particularly if the data subject is under 18. To make this decision you need to do a "balancing test". Legitimate interests is the most flexible lawful basis for processing and is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. It is our opinion that legitimate interest would be suitable for most of your processing as a recruitment company. The GDPR does not define what factors to take into account when deciding if your purpose is a legitimate interest. It could be as simple as it being legitimate to start up a new business activity, or to grow your business.

Therefore you would imagine that an individual who has applied directly for a role or has advertised their role on a job board would reasonably expect processing of their data. If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests. There are three elements to the legitimate interest's basis. It helps to think of this as a three-part test.

You need to consider:

- Purpose test: are you pursuing a legitimate interest?
- Necessity test: is the processing necessary for that purpose?
- Balancing test: do the individual's interests override the legitimate interest?

The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits. The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply. You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests. The biggest change is that you need to document your decisions on legitimate interests so that you can demonstrate compliance under the new GDPR accountability principle. You must also include more information in your privacy information." https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/#ib2

Looking at the three considerations; 1) We are pursuing a legitimate purpose, we are keeping data to find roles for the candidates there. 2) The process is necessary for purpose of finding people jobs, i.e. we need there contact details and other identifying data to contact candidates when a suitable role comes in. 3) We can judge that our purpose and necessity for holding information does not harm an individual's legitimate interests. Reasonable judgement would suggest that we fulfil the above 3 criteria and hence can change our lawful basis of retention to legitimate use. Effective 24th March 2022. Spinwell Global have changed our model of retention until further notice

Data Protection Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Data Protection Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

To ensure that use of personal information is controlled in accordance with the Data Protection Act 2018 and General Data Protection Regulations principles and that an individual's rights are respected.

Document Scope

This Directive applies to all Information Assets, including those relating to Company, customer and development information across the Company and where personal data is processed by external providers.

Responsibilities

Data Protection Officer:	Responsible for reviewing the details of potential or actual breaches of personal data notifications to ensure that these are referred back to the ICO. Additional requirements for notification may also arise from Personal Data Impact Assessments. The Data Protection Officer has direct responsibility for DP procedures, including Subject Access Requests.
IT staff:	For ensuring that data protection controls are implemented and records maintained.
Employees and contractors:	For ensuring that data protection controls are followed and for notifying the Data Protection Officer of concerns or breaches of personally identifiable information (PII). All staff employed by the Company are also responsible for ensuring that any personal data that is about them that is supplied by them is accurate and up to date.
Management:	Shall ensure their employees and contractors comply with this Directive.

Data Protection Introduction

The Company needs to collect and use certain types of information about staff and other individuals who come into contact with the Company in order to operate. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

This personal information must be dealt with properly, however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this is within the EU General Data Protection Regulation and the Data Protection Act.

A record of notification to the ICO is retained by the Data Protection Officer. The ICO Notification Handbook is used as the authoritative guidance for notification. This notification is reviewed

annually and update notifications are issued accordingly.

Any breach of the GDPR will be considered as a breach of the Disciplinary Policy and could also be considered a criminal offence, potentially resulting in prosecution.

Third parties working with or for the Company and who have or may have access to personal information will be expected to comply with this Directive. Third parties who require access to personal data will be required to sign a Confidentiality Agreement before access is permitted. This

will also include an agreement that the company can audit compliance with the Confidentiality Agreement.

The company is a data controller and/or a data processor as defined under GDPR and the Data Protection Act 2018.

Data Protection Principles

Any processing of personal data must be conducted in accordance with the following data protection principles of the Regulation, and company policies and procedures will ensure compliance.

Personal data must be processed lawfully, fairly and transparently.

The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' 'rights and freedoms'.

Information must be communicated to the data subject in an intelligible form using clear and plain language.

Management is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

All individuals are responsible for ensuring that any data held by the Company is accurate and up to date. Any data submitted by an individual to a Company, such as via a registration form, will be considered to be accurate at the time of receipt.

Employees or other individuals should notify the Company of any changes in personal information to ensure personal information is kept up to date. It is the responsibility of the Company to ensure that any notification of changes to personal information is implemented.

The Data Protection Officer is responsible for ensuring that all necessary actions are taken to ensure personal information is accurate and up to date. This should also take into account the volume of data collected, the speed with which it might change and any other relevant factors.

The Data Protection Officer will review, at least once a year, all the personal data processed by the Company, held in the Data Register. The Data Protection Officer will note any data that is no longer required in the context of the registered purpose and will ensure that it is appropriately removed and securely disposed of.

If a third party has provided inaccurate or out-of-date personal information, the Data Protection Officer is responsible for informing them that the personal information is inaccurate and/or out-of-date and will advise them that the information should no longer be used. The Data Protection Officer should also ensure that any correction to the personal information is passed on to the third party.

Personal Data

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

Where personal data is retained beyond the processing date, it will be encrypted in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed.

Personal data must be processed in a manner that ensures its security.

Appropriate technical and company measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Security controls will be subject to audit and review.

Compliance with this principle is contained in the Information Security Management System (ISMS), which has been developed in line with ISO/IEC 27001:2013 and the Security Policy set out in the ISMS.

Personal data shall not be transferred to a country or territory outside the European Union Member States 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.

The transfer of personal data outside of the EU Member States is prohibited unless one or more of the specified safeguards or exceptions apply.

An assessment of the adequacy is carried out by the data controller, taking into account the following factors:

- The nature of the information being transferred
- The country or territory of the origin, and final destination, of the information
- How the information will be used and for how long
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations and
- The security measures that are to be taken as regards the data in the overseas location.

Accountability

The GDPR states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR. As a result, controllers are required to keep all necessary documentation of all processing operations and implement appropriate security measures. They are also responsible for completing Data Processing Impact Assessments (DPIAs), complying with requirements for prior notifications, or approval from supervisory authorities and ensuring a Data Protection Officer is appointed, if required.

Data Subjects' Rights

Data subjects have the following rights regarding data processing and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To be informed about the mechanics of the automated decision-taking process that will significantly affect them
- Not to have significant decisions that will affect them taken solely by an automated process
- To sue for compensation if they suffer damage by any contravention of the GDPR

- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data
- To request the ICO to assess whether any provision of the GDPR has been contravened
- The right for personal data to be provided to them in a structured, commonly used and machine-readable format and the right to have that data transmitted to another controller
- The right to object to any automated profiling without consent
- Data subjects may make data access requests. These are reviewed by the Data Protection Officer and processed so that the procedure ensures that its response to the data access request complies with the requirements of the regulations.

Complaints

A Data Subject has the right to complain at any time to the Company if they have concerns about how their information is used. If they wish to lodge a complaint, this should be directed to the Data Protection Officer.

A Data Subject also has the option to complain directly to the Information Commissioner's Office. Details of the options for lodging a complaint should be provided.

Consent

'Consent' is taken by the Company to mean that agreement to the processing of personal data has been explicitly and freely given and that this consent is specific, informed and an unambiguous indication of the data subject's wishes. The consent of the data subject can be withdrawn at any time.

Consent is also taken by the Company on the basis that it has been given by the data subject who is fully informed of the intended processing and is in a fit state of mind and without undue pressure to give consent being applied.

There must be some active communication between the parties which demonstrates active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

Consent to process personal and sensitive data is obtained routinely using standard consent documents. This may be through a contract of employment or during initial induction.

Data Security

Company staff that are responsible for any personal data must keep it securely and ensure that it is not disclosed under any conditions to any third party unless that third party has been specifically authorised to receive that information and has entered into a confidentiality agreement.

Personal data should be accessible only to those who need to use it and access may only be granted in line with the Access Control Aspects Policy. You should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- In a lockable room with controlled access; and/or
- In a locked drawer or filing cabinet; and/or
- If computerised, it must be password protected in line with the *Access Control* and *Secure Systems & Development Aspects Directives*
- Stored on encrypted removable media in line with the *Cryptography Aspects Directive.*

Care must be taken to ensure that PC screens and terminals are not visible except to authorised staff. Staff must review the Acceptable Use Aspects Directive before they are given access to Company information.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit (written) authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving.

Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed. Because of the increased risk, all staff must be specifically authorised to process data off-site.

Data Access Rights

Data subjects have the right to access any personal data (i.e. data about them) which is held in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references and information obtained from third parties about that person.

Disclosure of Data

The Company ensures that personal data is not disclosed to unauthorised third parties including family members, friends, government bodies and, in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not a disclosure of the information is relevant to, and necessary for, the conduct of business operations.

GDPR permits a number of exemptions where certain disclosure without consent is permitted, as long as the information is requested for one or more of the following purposes:

- To safeguard national security
- Prevention or detection of crime including the apprehension or prosecution of offenders
- Assessment or collection of tax duty
- Discharge of regulatory functions (includes health, safety and welfare of persons at work)
- To prevent serious harm to a third party
- To protect the vital interests of the individual - this refers to life and death situations.

Requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

Data Retention and Disposal

Personal data may not be retained for longer than it is required. Some data will be kept for longer periods than others.

Personal data must be disposed of in a way that protects the 'rights and freedoms' of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion, or obfuscation of personally identifiable data).

GDPR Risk Assessment

The Company needs to ensure that it is aware of any risks associated with the processing of all types of personal information. A Risk Assessment procedure has been implemented and is used by the Company to assess any risk to individuals during the processing of their personal information.

Assessments will also be completed for any processing that is undertaken on their behalf by any third-party organisation. Through the application of the Risk Assessment procedure, the Company ensures that any identified risks are managed appropriately to reduce the risk of non-compliance.

Where the processing of personal information may result in a high risk to the 'rights and freedoms' of natural persons, the Company will complete a data protection impact assessment, prior to conducting the processing, to ensure the personal information is protected. This assessment may also be used to apply to a number of similar processing scenarios with a similar level of risk.

Where, as a result of a Data Protection Impact Assessment, it is clear that the Company will process personal information in a manner that may cause damage and/or distress to the data subjects, the Data Protection Officer must review the process before the Company proceeds to process the information. If the Protection Officer decides that there are significant risks to the data subject they will escalate to the ICO for final guidance. The Company will apply selected controls for the ISO 27001 Annex A to reduce risk. This also references the Company's risk acceptance criteria and the requirements of the GDPR and The Data Protection Act 2018.