

Bowlers Data Protection Policy (GDPR)

**Purpose**

Bowlers is committed to being transparent about how it collects and uses the personal data for its workforce, and to meeting its data protection obligations. This policy sets out Bowlers commitment to data protection, and individual rights and obligations in relation to personal data in accordance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018.

This policy applies to the personal data of; the recruitment process including internal selection processes, job applicants, employees, workers, contractors, volunteers, interns, apprentices, and former employees, referred to as HR-related personal data. This policy also relates to any monitoring of employees. This policy does not apply to the personal data of clients or other personal data processed for business purposes which is held within a separate document and forms the business relationship with Bowlers clients.

Bowlers has appointed a senior member of the team as the person with responsibility for data protection compliance within Bowlers. They can be contacted through your Line Manager. Questions about this policy, or requests for further information, should be directed to them through your Line Manager.

**Definitions**

**"Personal data" is** any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.

**"Special categories of personal data"** means information about an individual’s, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

**"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

**Data protection principles**

Bowlers processes HR-related personal data in accordance with the following data protection principles:

* Bowlers processes personal data lawfully, fairly and in a transparent manner.
* Bowlers collects personal data only for specified, explicit and legitimate purposes.
* Bowlers processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
* Bowlers keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
* Bowlers keeps personal data only for the period necessary for processing.
* Data relating to unsuccessful job applicants will only be retained for a period of one year.
* Bowlers adopts appropriate measures to make sure that personal data is secure, and

protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Bowlers tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where Bowlers relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where Bowlers processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

Bowlers will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the; employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file (in both hard copy and electronic format), and on HR systems. The periods for which Bowlers holds HR-related personal data are contained in its privacy notices to individuals.

Bowlers keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

**Individual rights**

As a data subject, individuals have a number of rights in relation to their personal data.

**Subject access requests**

Individuals have the right to make a subject access request. If an individual makes a subject access request, Bowlers will tell them:

* whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual.
* to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers.
* for how long their personal data is stored (or how that period is decided).
* their rights to rectification or erasure of data, or to restrict or object to processing.
* their right to complain to the Information Commissioner if they think Bowlers has failed to comply with their data protection rights; and
* whether or not Bowlers carries out automated decision-making and the logic involved in any such decision-making.

Bowlers will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

To make a subject access request, the individual should send the request through their Line Manager by completing a Subject Access Request Form. Bowlers may need to ask for proof of identification before the request can be processed. Bowlers will inform the individual if it needs to verify their identity and the documents it requires.

Bowlers will normally respond to a request within a period of one month from the date it is received. In some cases, such as where Bowlers processes large amounts of the individual's data, it may respond within three months of the date the request is received. Bowlers will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, Bowlers is not obliged to comply with it. Alternatively, Bowlers can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which Bowlers has already responded. If an individual submits a request that is unfounded or excessive, Bowlers will notify them that this is the case and whether or not it will respond to it.

**Other rights**

Individuals have a number of other rights in relation to their personal data. They can require the Bowlers to:

* rectify inaccurate data.
* stop processing or erase data that is no longer necessary for the purposes of processing.
* stop processing or erase data if the individual's interests override Bowlers legitimate grounds for processing data (where Bowlers relies on its legitimate interests as a reason for processing data).
* stop processing or erase data if processing is unlawful; and
* stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override Bowlers legitimate grounds for processing data.

To ask Bowlers to take any of these steps, the individual should send the request to the Data Controller.

**Data security**

Bowlers takes the security of HR-related personal data seriously. Bowlers has internal policies and controls in place to protect personal data against; loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where Bowlers engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and Bowlers measures to ensure the security of data.

**Impact assessments**

Some of the processing that Bowlers carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, Bowlers will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

**Data breaches**

If Bowlers discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Bowlers will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

**International data transfers**

Bowlers will not transfer HR-related personal data to countries outside the EEA.

**Individual responsibilities**

Individuals are responsible for helping Bowlers keep their personal data up to date. Individuals should let Bowlers know if data provided to Bowlers changes, for example if an individual changes their address or changes their bank details.

Individuals may have access to the personal data of other individuals and of Bowlers customers and clients in the course of their, employment, Contract, volunteer period, internship or apprenticeship. Where this is the case, Bowlers relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

* to access only data that they have authority to access and only for authorised purposes.
* not to disclose data except to individuals (whether inside or outside Bowlers) who have appropriate authorisation.
* to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction).
* not to remove personal data, or devices containing or that can be used to access personal data, from Bowlers premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.
* not to store personal data on local drives or on personal devices that are used for work purposes; and
* to report data breaches of which they become aware to a Director immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under Bowlers Disciplinary Procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

**Training**

Bowlers will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Data Policy – Business Related Data

**Purpose**

Bowlers is committed to being transparent about how it collects and uses the personal data of its clients, suppliers and associates and to meeting its data protection obligations. This policy sets out Bowlers commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of clients or other personal data processed for business purposes and relates to Bowlers Data Protection Policy held within this handbook.

Bowlers has appointed a senior member of the team as the person with responsibility for data protection compliance within Bowlers. They can be contacted through your Line Manager. Questions about this policy, or requests for further information, should be directed to them through your Line Manager.

During your work, as an employee of Bowlers, you may encounter or use confidential information about Bowlers own employees, clients and customers, for example their names and home addresses. The Data Protection Act 2018 contains principles affecting personal records.

Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data, for example to form part of a structured filing system. It includes personal data stored or processed within Bowlers premises, or employees when working remotely including homeworking.

The purpose of these rules is to ensure you do not breach the Act. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from your Line Manager or Bowlers Data Protection Officer/Data Controller.

You should be aware that you can be criminally liable if you knowingly or recklessly disclose personal data in breach of the Act. A serious breach of data protection is also a disciplinary offence and will be dealt with under Bowlers Disciplinary Procedure. If you access another employee’s personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal.

Most companies may need to register with the Information Commissioner’s Office (ICO). If this is the case, then a certificate will be issued to be displayed. Any Bowlers using CCTV will need to be registered.

**The data protection principles**

There are eight data protection principles that are central to the Act. Bowlers and all its employees must comply with these principles always in its information-handling practices. In brief, the principles say that personal data must be:

1. Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data. The conditions are either that the employee has given consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of the employee and consists of information relating to:

* race or ethnic origin.
* political opinions and trade union membership.
* religious or other beliefs.
* physical or mental health or condition.
* sexual life.
* criminal offences both committed and alleged.

2. Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.

3. Adequate, relevant and not excessive to ensure they do not contain a backlog of out-of-date information and to check there is a sound business reason requiring information to continue to be held.

4. Accurate and kept up to date. Bowlers cannot be held responsible for any errors unless they have been notified of the relevant change.

5. Not kept for longer than is necessary. Various categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data which Bowlers decides it does not need to hold for a period will be destroyed after one year.

6. Processed in accordance with the rights of employees under the Act.

7. Secure, technical and Bowlers measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data. Personel files are confidential and are stored in locked filing cabinets. Only authorised staff will have access to these files. Files will not be removed from their normal place of storage without good reason. Data stored on diskettes or other removable media will be kept in locked filing cabinets. Data held on computer will be stored confidentially by means of password protection, encryption or coding and again only authorised employees have access to that data. Bowlers has network backup procedures to ensure that data on computer cannot be accidentally lost or destroyed.

8. Not transferred to a country or territory outside the European Economic Area (EEA) unless that country ensures an adequate level of protection for the processing of personal data.

**Data protection: subject access to data**

Under the terms of the Data Protection Act 2018, “subject access” is an individual’s right to gain access to data (if any) held about themselves by Bowlers in electronic format and/or manual records.

Any individual, an employee or a client who wishes to exercise this right has to make an application in writing; this should be done by asking the individual to complete the Subject Access Request Application Form.

Bowlers needs to be assured of an applicant’s identity before relevant data is released.

The individual making the request must be made aware that Bowlers may require a period of one month in which to provide the required information.

If you wish to make a complaint that the rules are not being followed in respect of personal data the Bowlers holds about you, you should raise the matter with the Data Protection Officer. If the matter is not resolved to your satisfaction this needs to be raised with the Information Commissioner’s Office.

**Your individual obligations in relation to personal information**

You should ensure you comply with the following guidelines at all times:

* Do not give out confidential personal information except to the data subject. In particular, it should not be given to someone from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this.
* Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.
* Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.
* If you receive a request for personal information about another employee, you should forward this to your Line Manager who will be responsible for dealing with such requests.
* Ensure any personal data you hold is kept securely, either in a locked filing cabinet or, if computerised, it is password protected.
* Compliance with the act is your responsibility. If you have any questions or concerns about the interpretation of these rules, take this up with the Data Protection Officer/Data Protection Controller.

**Fair and lawful processing**

The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, who the data controller’s representative is, the purpose for which the data is to be processed by Bowlers and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain specific conditions have to be met. These include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. In some cases, the data subject’s explicit consent to the processing of such data will be required.

**Processing for limited purposes**

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

**Adequate, relevant and non-excessive processing**

Personal data should only be collected to the extent that it is required for the specific purpose notified for the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

**Accurate data**

Personal data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate, and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

**Timely processing**

Personal data should not be kept for longer than is necessary for the purpose. This means that data should be destroyed or erased from Bowlers systems when it is no longer required.

**Processing in line with data subject’s rights**

Data must be processed in line with data subjects’ rights. Data subjects have a right to:

* request access to any data held about them by a Data Controller.
* prevent the processing of their data for direct marketing purposes.
* ask to have inaccurate data amended.
* prevent processing that is likely to cause damage or distress to themselves or anyone else.

**Data security**

Bowlers must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The Act requires Bowlers to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

* Confidentiality means that only people who are authorised to use the data can access it.
* Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
* Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the central computer system instead of individual PCs.

**Security procedures include:**

* Entry controls – any stranger seen in entry-controlled areas should be reported.
* Secure lockable desks and cupboards – desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
* Methods of disposal – paper documents should be shredded. Portable devices should be physically destroyed when they are no longer required.
* Equipment – data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is

left unattended.

**Staff removal of data**

The Information Commissioner has stated that it is an offence under the Data Protection Act to take client records containing person information to a new job without the express permission in writing of every person on the list. This is a criminal offence and will attract a hefty fine for the individual committing the act. Bowlers will most likely be duty bound to inform the Information Commissioner if they consider a breach of the Act has occurred.