

ACHILLES INFORMATION LIMITED - DATA PROTECTION POLICY

POLICY STATEMENT

- Achilles services are all about data management. Therefore great importance is placed on managing these services professionally, with due regard for data quality, integrity, security, privacy and the rights of individuals, which includes personal data as well as operational data.
- Achilles retains and processes information about its employees or potential employees, contractors, assessors and auditors for both administrative and operational purposes. It also holds a limited amount of personal data in the supplier management systems, which has been entered by the customers themselves in responses to questionnaires or other data entry screens, and in customer relationship management systems. Some information is also held resulting from assessments and audits of suppliers.
- All Achilles staff and others, on our behalf, who process or use such information, will comply with the Eight Data Protection Principles which are set out in the Data Protection Act 1998. In brief this means that such personal data will:
 - Be processed fairly and lawfully.
 - Be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes.
 - Be adequate, relevant and not excessive for the purposes.
 - Be accurate and where necessary be kept up-to-date.
 - Not be kept for longer than necessary for the purposes.
 - Be processed in accordance with the data subject's rights.
 - Be protected from unauthorised processing, accidental loss, destruction or damage.
 - Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.
- Achilles will provide the necessary resources and training to enable continuing compliance.

ARRANGEMENTS

Data Controllers

- Achilles Information Limited assumes the responsibility as Data Controller for all personal data for employees or potential employees, assessors and auditors, for any personal data in customer relationship management systems, backed up and historical databases, and within assessment and audit reports. However they jointly assume the responsibility of Data Controller with each customer who himself enters and maintains data in our databases by means of questionnaires or other data entry screens.

Notification of Data Held

- Achilles Information Limited has registered with the Information Commissioners Office for how the data held within the supplier management systems, customer relationship systems and assessment and auditing systems is disclosed to others as part of the operational process. This data may also be used for advertising, marketing, public relations, accounts and record keeping.
- Employee personal data held by Achilles is maintained for the purposes of normal administration of staff or potential staff, typically purposes such as payroll, time off, competencies, training, career development and recruiting. Personal data concerning contractors' personnel is held and used for contractor management.

Managerial Responsibilities

- As well as accepting the responsibilities of members of staff as detailed below, managers and directors have the added responsibility for ensuring that all staff under their control are made aware of and understand the Staff Responsibilities.

Staff Responsibilities

- All staff will ensure that all personal information which they provide to Achilles in connection with their employment, is accurate and up-to-date, and must inform the relevant HR department of any changes required.
- Staff holding or processing personal information about employees may only disclose such information to someone outside of the organization for the following reasons:
 - To 3rd parties who process data on behalf of Achilles; ie organizations providing services such as payroll.
 - As required by law, in which case the information must be passed directly to a constable, whose identity has been validated. All requirements of this nature must be passed to the HR Manager or Company Secretary in the first instance.
 - Where the information is about an assessor or auditor, and the related assessment scheme requires disclosure to scheme management committees for the validation of their competence in relation to defined assessment or audit protocols.
- Staff holding or processing personal information about employees may disclose such information to someone within the organization, but then only for normal administrative purposes on a strictly need-to-know basis. If the disclosure is to be made remotely (telephone, fax or email, or letter) then the identity of the recipient must be assured.
- Staff must be made aware that information about a person's physical or mental health, ethnicity or race, political or religious views, trade union membership, sexual life, or criminal record is sensitive personal data under The Act. Such information can only be collected and processed as required by law, eg with the subject person's express consent. Such information may only be collected and processed by HR departments, and then only where it is absolutely essential, and maintained no longer than necessary.
- Operations staff, assessors and auditors must under no circumstances record sensitive personal data about anybody. In particular, they must take care not to do this inadvertently when creating or updating records in customer relationship management systems, assessment or audit reports, or in the notes created for generating such reports.
- Staff shall ensure that all personal data is kept securely in the office; this means:
 - Hard copy, removable media and portable computing systems containing such data (including synchronised files) will be kept under lock and key when not in use.
 - Any computer systems holding such data (including portable computing systems) will be protected by means of a strong password that is regularly changed, with permissions set to restrict access to authorised staff only. Passwords will be kept secret by users, and not shared for any purpose.
 - Computer based data shall be further protected from intrusion and damage by means of effective firewalls, up-to-date virus scanning and regular backups, with backup media itself protected against fire and theft, or unauthorised access.
 - Personal data will not be taken home for home working purposes (in any format) without the express permission of the HR Manager or a director (or as defined in the next clause), and then only when it may be stored with security equivalent to that of the office. If left in a car, this should only be for minimum periods, when it must be placed in the locked boot area of the car. Under no circumstances should it be left in a car overnight.
 - Auditor and Assessor notes or other related documentation containing personal data may be stored at the home of the auditor or assessor. The auditor or assessor must agree that his or her storage arrangements will be subject to audit by Achilles.

Sensitive Personal Data

- Achilles HR departments may process sensitive personal data, but only about a person's health, disabilities, race or ethnic origin for the administration of the sickness and absence

policy or the equal opportunities policy, or for the provision of facilities to meet an individual's specialist needs.

System Specification, Design and Configuration

- Those responsible for creating, updating or configuring supplier management systems and customer relationship systems, including manual systems, have the responsibility for ensuring that if personal data is to be processed by the system and its users, then full compliance with The Act is accomplished, throughout the lifecycle of the data. In particular, data available on a global basis must not include personal data, without the consent of the data subject.

RETENTION OF DATA

- Achilles keeps various types of information for differing lengths of time, depending on legal and operational requirements:
 - For employee personal data within the HR department, this is typically for up to 10 years after a person has left the employ of Achilles.
 - Personal data concerning unsuccessful candidates for employment (either full time or temporary,) will be disposed of within 3 months of the completion or cancellation of the related recruitment process.
 - Data concerning the performance of potential contractors should be kept no longer than 2 years.
 - Where possible, personal data within expired records of supplier management systems, should be deleted 2 years after the expiry date.
 - Where possible, data in customer relationship management systems for customers should be retained for no longer than 4 years, after which they may be archived for an additional 4 years before being deleted.
 - Assessors and auditors are required to keep their notes for 3 years, but the notes should not retained for more than 5 years, after which they must be securely destroyed.

DISPOSAL OF PERSONAL DATA

- The following methods will be employed to dispose of personal data when it has reached the end of its agreed retention time:
 - Hard copy – by secure shredding.
 - Floppy discs and CDROMs – by physical destruction of the media, before normal disposal.
 - Network Storage – by normal deletion (recovery of the space by normal usage is likely to over-write the old data segments in a reasonable time).
 - Portable computing systems - deletion plus immediate emptying of the recycle bin if used by the system. However, users who regularly load personal data onto their laptops, should have a suitable file shredding utility installed, which should be run weekly.
 - Any computers which are to be disposed of complete with their hard drives, and which have had personal data installed are to have the hard drive content shredded (by means of a suitable utility) before reformatting.
 - Individual hard drives that are to be disposed of, must either be physically wrecked, or have their content shredded before disposal.

RIGHTS TO ACCESS INFORMATION

- Employees, auditors and assessors and other data subjects have the right to access any personal data that is being kept about them either on computer or in structured and accessible manual files. Any person may exercise this right by submitting a request in writing to the HR Manager. Achilles reserves the right to charge a small fee (as allowed by The Act) for granting of such access.
- Achilles will endeavor to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is good reason for

delay. In such cases, the reason for the delay will be explained in writing by the HR Manager to the person making the request.

- Where necessary the identity of the person making the request will be validated before disclosing the requested information. Requests will not be accepted on behalf of others, unless power of attorney can be demonstrated.